UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL ADMINISTRADA UTILIZANDO UN FIREWALL FORTIGATE 1500D PARA LA PROTECCIÓN DE LA RED LAN DE LA UNIVERSIDAD NACIONAL DE TRUJILLO”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

PEREZ LEYVA, MARCO RODO

Villa El Salvador

2017

DEDICATORIA

Este informe está dedicado a mis padres por todo el apoyo, amor y comprensión brindados en el transcurso de este largo camino; igualmente a mis hermanos, que dieron todo de sí para verme como profesional, y principalmente deseo agradecer a Dios por la oportunidad dada.

AGRADECIMIENTO

Este proyecto es el resultado del esfuerzo conjunto de todos los que formamos el grupo de trabajo. Por esto agradezco al ingeniero de proyectos, Ing. Harold Angulo, a mi compañero Ing. Alfonso Ibáñez y mi persona, quienes a lo largo de este tiempo han puesto a prueba sus capacidades y conocimientos en el desarrollo de este nuevo plan de seguridad el cual ha finalizado llenando todas nuestras expectativas. A mis padres quienes a lo largo de toda mi vida han apoyado y motivado mi formación académica, creyeron en mí en todo momento y no dudaron de mis habilidades. A mis profesores a quienes les debo gran parte de mis conocimientos, gracias a su paciencia y enseñanza y finalmente un eterno agradecimiento a esta prestigiosa universidad la cual abrió sus puertas a jóvenes como nosotros, preparándonos para un futuro competitivo y formándonos como personas de bien.

IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL ADMINISTRADA UTILIZANDO UN FIREWALL FORTIGATE 1500D PARA LA PROTECCIÓN DE LA RED LAN DE LA UNIVERSIDAD NACIONAL DE TRUJILLO

ÍNDICE GENERAL

DEDICATORIA **IV**

AGRADECIMIENTO **V**

INDICE **VII**

INDICE DE TABLAS **X**

ÍNDICE DE FIGURAS **X**

INTRODUCCIÓN **12**

ÍNDICE

1. CAPITULO I: PLANTEAMIENTO DEL PROBLEMA **14**

1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA **14**

1.2 JUSTIFICACIÓN DEL PROBLEMA 15

1.3 DELIMITACIÓN DEL PROYECTO 17

1.3.1 Delimitación Espacial 17

1.3.2 Delimitación Temporal 17

1.4. FORMULACIÓN DEL PROBLEMA 17

1.4.1 Problema Principal 17

1.4.2 Problemas Específicos 17

1.5 OBJETIVOS 18

1.5.1 Objetivo General 18

1.5.2 Objetivos Específicos 18

2. CAPÍTULO II: MARCO TEÓRICO **19**

2.1. ANTECEDENTES DE LA INVESTIGACIÓN 19

2.2. BASES TEÓRICAS 22

2.2.1 SEGURIDAD PERIMETRAL ADMINISTRADA (SPA) 22

2.2.2 LAN (RED DE ÁREA LOCAL) 24

2.2.3 TECNOLOGÍA UTM (FIREWALL) 29

2.2.3.1 Modos Proxy 30

2.2.3.2 Modo Transparente: 30
2.3 MARCO CONCEPTUAL 31
2.3.1 FUNDAMENTOS TEÓRICOS DE SEGURIDAD EN REDES 31
2.3.1.1 Seguridad Informática 32
2.3.1.2 Amenazas 34
2.3.1.3 Vulnerabilidades 36
2.3.1.4 Mecanismo 37
2.3.1.5 Modelos de Seguridad 39
2.3.1.6 Seguridad en entidades 39
2.3.1.7 Políticas de Seguridad Informática 40
2.3.1.8 Políticas y Procedimientos 41
2.3.1.9 Técnicas de Ataques y Protecciones 42
2.3.1.10 Protecciones 43
2.3.1.11 Tecnologías de Seguridad Informática 44
2.3.1.12 VPN (Red Privada Virtual) 51
2.3.1.13 Modelos de Autenticación 53
2.3.1.14 Sistemas de Detección de Intrusos (IDS) 55
2.3.1.15 Sistemas de Detección de Intrusos para Host (HIDS) 55
2.1.3.16 Sistemas de Detección de Intrusos para Red (NIDS) 56
2.1.3.17 Detección de Anomalías 56
2.1.3.18 Detección de Usos Indebidos 57
2.3.1.19 Seguridad Física de Red 57
2.3.1.20 UTM (Unified Threat Management) 60
2.3.2 Análisis Solución de Implementación: FortiGate de Fortinet 63
2.3.2.1 FORTALEZAS 65
2.3.2.2 DEBILIDADES: 65
2.3.2.3 Fortiguard Distribution Network (FDN) 67
2.3.2.4 FortiGuard Center 67
2.3.2.5 FortiGate 69
2.3.2.6 Administración del Sistema 74
3. CAPÍTULO III: DESCRIPCIÓN DEL MODELO 93
3.1. ANÁLISIS DEL MODELO 93
3.1.1 Topología Inicial 93

3.1.2 Requerimientos 95
3.1.3 Propuesta de solución Firewall 97
3.1.3.1 Descripción técnica de equipos a instalar 97
3.1.3.2 Costos de la solución 100
3.1.4 Diagrama de Actividades Secuenciales 101
3.1.4.1 Requerimientos Físicos FORTINET 102
3.1.4.2 Requerimientos para la configuración 103
3.1.4.3 Topología a Implementar 104
3.1.4.4 Cronograma 106
3.1.4.5 Plan de Implementación 107
3.1.4.6 Plan de Migración 108
3.2 CONSTRUCCIÓN DEL MODELO 110
3.2.1 FortiGate 1500D 110
3.2.1.2 Licenciamiento 110
3.2.1.3 Información del Sistema 111
3.2.1.4 Interfaces Configuradas 112
3.2.1.5 Configuración de Administración 113
3.3 REVISIÓN Y CONSOLIDACIÓN DE RESULTADOS 121
3.3.1 CPU y Memoria 121
3.3.2 Verificación del estado de las interfaces 122
3.3.3 Pruebas de Conectividad Básica 127
3.3.4 Pruebas de Publicación 128
3.3.5 Pruebas de Política (Acceso a servicios) 129
CONCLUSIONES **130**
RECOMENDACIONES **131**
BIBLIOGRAFÍA **133**

INDICE DE TABLAS

Tabla 1: Costos de los equipos FortiGate (Principal y Spare)

Tabla 2: Costo de Instalación y configuración del equipo FortiGate

Tabla 3: Costo de Capacitación del equipo FortiGate

Tabla 4: Diagrama de Actividades Secuenciales

Tabla 5: Cronograma de actividades

Tabla 6: Plan de Migración

ÍNDICE DE FIGURAS

Figura 1: Red de Seguridad Perimetral

Figura 2:Comunicación de host locales

Figura 3: Comunicación de host en distinta redes locales

Figura 4: Gestión Unificada de Amenazas

Figura 5: Cuadrante mágico para UTMs realizados por la entidad Gartner

Figura 6: Principales Tecnologías y ámbitos del Fortinet

Figura 7: Servicio FortiGuard

Figura 8: Estado del sistema en el FortiGate

Figura 9: Configuración Modo NAT / Router.

Figura 10: Fase 1 – VPN IPSec

Figura 11: Fase 2 – VPN IPSec

Figura 11: Topología Inicial de Red Interna de la Universidad Nacional de Trujillo

Figura 12: Configuración de VLANs de la Red Lan del Cliente.

Figura 13: Datashep FortiGate 1500 D

Figura 14: 2U Rack mount.

Figura 15: FortiGate instalado en el gabinete

Figura 16: Fuentes de alimentacion del equipo Fortigate

Figura 17: Topología Final de la red LAN de la Universidad Nacional de Trujillo
Figura 18: Caracteristicas de Licencia
Figura 19: Descripción y Registro de Licenciamiento
Figura 20: Información del Sistema
Figura 21: Puertos Conectados del FortiGate
Figura 22: Direccionamiento IP
Figura 23: Acceso para la Gestión del FortiGate
Figura 24: Puertos de Enlaces (Default Route)
Figura 25: Configuracion SNMP (Protocolo Simple de Administración de Red)
Figura 26: Cuentas de Administración
Figura 27: Perfiles de Admistración
Figura 28: Politica de Navegacion – NAT
Figura 29: Politicas de Navegacion hacia Internet
Figura 30: Bloqueo de Categorías
Figura 31: Configuración Antivirus
Figura 32: Control de Aplicaciones
Figura 33: Configuración IPS
Figura 34: Consumo de CPU y Memoria
Figura 35: Puerto 17 – Diagnostico
Figura 36: Puerto 18 – Diagnostico
Figura 37: Puerto 19 – Diagnostico
Figura 38: Puerto 20 – Diadnostico
Figura 39: Conectividad hacia la Pagina Google, por IP y DNS.
Figura 40: Oficina General de Adminision de la Universidad Nacional de Trujillo
Figura 41: Conectividad a la web admisionunt.info
Figura 42: Control de acceso hacia Internet

INTRODUCCIÓN

La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla en las computadoras distribuidas. En este tipo de sistemas resulta muy sencillo para un usuario experto acceder de forma no autorizada a datos de carácter confidencial.

Toda organización debe estar a la vanguardia de los procesos de cambio. Estos procesos deben disponer de información continua y confiable en el tiempo, esto constituye una ventaja fundamental.

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red LAN (Red de Área Local) son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico.

El presente proyecto de ingeniería propone el desarrollo y la implementación de aspectos relacionados a la solución de una seguridad perimetral

administrada en la red LAN (Red de Área Local) de la Universidad Nacional de Trujillo, lo que permitirá a la entidad y a los usuarios de la red, tener una mayor confianza, seguridad y efectividad en los procesos internos.

1 CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

La seguridad en los sistemas de comunicaciones no solo es un problema tecnológico sino que se extiende sobre la capacidad y honorabilidad de las personas y eficiencia de los procesos; para minimizar los riesgos de seguridad en las redes de comunicaciones, es imprescindible un servicio profesional especializado y experto, que transforme la defensa en un proceso continuo y dinámico. En la actualidad la Universidad Nacional de Trujillo, no controla adecuadamente el nivel de seguridad perimetral, protección y control de ataques a nivel de red interno y externo, provocando que los sistemas se hallen susceptibles a ataques informáticos; para la red LAN (Red de Área Local) se realizará un análisis de la situación actual de la entidad, para luego implementar una solución de seguridad perimetral administrada de tal manera de que se pueda analizar los servicios en su plataforma de red LAN (Red de Área Local), tomando en cuenta aspectos como la infraestructura, los servicios, los protocolos, las aplicaciones que maneja la red y la forma de acceso al Internet, a la Intranet y a la Extranet. La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de cómputo son

actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico.

En conclusión, el problema consiste en abordar los temas fundamentales en el área de seguridad perimetral, a fin de proponer una metodología que facilite el diagnóstico e implementación de la solución de seguridad perimetral administrada en la red LAN (Red de Área Local) de la Universidad Nacional de Trujillo.

1.2 JUSTIFICACIÓN DEL PROBLEMA

Las amenazas de seguridad que enfrentan las redes de datos en Perú son suficientes para pensar en las posibles soluciones que disponemos en la actualidad para enfrentar dichas amenazas, esto nos plantea el problema de cuál es la mejor manera para resolver esta situación. Estas intrusiones no deseadas pueden ser detenidas siempre y cuando las organizaciones definan e implementen de una manera clara sus opciones en seguridad perimetral, esto en concordancia con las políticas de seguridad previamente establecidas.

La seguridad en las redes de datos depende directamente de las amenazas a las que estén expuestas, con el acceso a Internet esa posibilidad se incrementa en forma exponencial. El ataque a una red de datos requiere por parte de quien lo realiza de mucho tiempo, conocimiento y paciencia. Curiosamente esas son las mismas características que debe tener quien la defiende, en realidad el perfil del administrador de una red y de un hacker son muy parecidos, solo cambian sus intereses.

El nivel de amenaza de la Universidad Nacional de Trujillo está orientada básicamente a la información con la que cuenta de sus alumnos, y cualquier acceso no autorizado o no detectado para llegar a dicha información puede ser de alto riesgo o tener un alto nivel de impacto en la imagen de la entidad. Por tanto, es indispensable que se establezcan niveles y mecanismos básicos de control y seguridad para proteger la red de datos y la información que circula a través de ella.

En un alto porcentaje las organizaciones peruanas, carecen de profesionales y recursos en el tema de seguridad de redes de datos y por tal razón permanentemente están expuestas tanto a amenazas internas originadas desde el interior de la organización por medio de sus usuarios, como amenazas externas originadas por fuera de la organización, esto último se presenta especialmente cuando una organización se interconecta con otras organizaciones o con la Internet; por lo anterior el desarrollo del presente trabajo busca reforzar las políticas de seguridad de la Universidad Nacional de Trujillo y disminuir los riesgos de seguridad presentes para los recursos tecnológicos de la organización, fortaleciendo la protección perimetral de la infraestructura tecnológica frente a amenazas de seguridad, a través de un firewall, sistema de protección de intrusos, el control de la navegación de los usuarios al interior de la organización, control de aplicaciones y la prestación de servicios de acceso seguro a través de VPN (Red Privada Virtual).

1.3 DELIMITACIÓN DEL PROYECTO

1.3.1 Delimitación Espacial

El presente proyecto, se desarrolló en la Universidad Nacional de Trujillo, que está ubicada en la Avenida Juan Pablo II SN Ciudad, perteneciente a la ciudad de Trujillo – La Libertad, Perú.

1.3.2 Delimitación Temporal

El proyecto se implementó el 15 de Agosto del año 2016.

1.4. FORMULACIÓN DEL PROBLEMA

1.4.1 Problema Principal

¿Cómo desarrollar un diseño para ofrecer sistemas de información en redes, que permita conservar la operación de un sistema seguro, confiable, flexible, de alto desempeño y que brinde integridad de la información?

1.4.2 Problemas Específicos

- ✓ ¿Cómo analizar la seguridad informática en las redes académicas de la Universidad Nacional de Trujillo?
- ✓ ¿Cómo diagnosticar e identificar las vulnerabilidades de la seguridad informática de las redes académicas de la Universidad Nacional de Trujillo?
- ✓ ¿Cómo definir una arquitectura de seguridad en base a la plataforma de redes y comunicaciones de la Universidad Nacional de Trujillo?
- ✓ ¿Cómo establecer procesos esquematizados que cumplan con el desarrollo de la seguridad perimetral de la Universidad Nacional de Trujillo?

- ✓ ¿Cómo instalar el equipo FortiGate 1500 D y como protegerá la seguridad perimetral de las redes académicas de la Universidad Nacional de Trujillo?

1.5 OBJETIVOS

1.5.1 Objetivo General

Implementación de una solución de seguridad informática para la red académica de la Universidad Nacional de Trujillo.

1.5.2 Objetivos Específicos

- Analizar y estudiar la situación de seguridad informática en las redes de la Universidad Nacional de Trujillo.
- Diagnosticar las vulnerabilidades de seguridad informática de las redes de la Universidad Nacional de Trujillo y definir los posibles ataques e infecciones a prevenir dentro de la misma.
- Definir una arquitectura de seguridad en base a la plataforma de redes y comunicaciones de la entidad.
- Establecer procesos esquematizados que cumplan con el desarrollo de una red de seguridad perimetral para la Universidad Nacional de Trujillo.
- Instalar el equipo de seguridad FortiGate 1500D, para la protección perimetral de las redes de la Universidad Nacional de Trujillo.

2 CAPÍTULO II: MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Lacayo, A. (2004), en su tesis: ‘‘Análisis e implementación de un esquema de seguridad en redes para la Universidad de Colima’’ de la Universidad De Colima - México. Concluye lo siguiente: “El establecimiento de un esquema de seguridad, no es tarea de una sola persona, todos los integrantes de la institución deben ser involucrados y las políticas de seguridad deben implementarse gradualmente, e ir acompañadas de un programa de concienciación.

DIGESET es la dependencia encargada de la distribución y administración de la red externa e interna de la Universidad de Colima, por lo tanto, debe incorporar la toma de decisiones basada en el análisis de riesgos para responder a tres preguntas básicas sobre la seguridad, estas son: ¿Qué quieren proteger?, ¿Contra quién (o qué) quieren protegerse? y ¿Cómo lo quieren proteger? Para ello se implementó la tecnología UTM (Gestión

Unificada de Amenazas) que permitió obtener resultados importantes para el esquema de seguridad actual de la Universidad de Colima.

Este tipo de tecnología permitió que la Universidad de Colima, tenga un sistema protegido contra ataques de denegación de servicio y un control de acceso de los estudiantes hacia la red interna de la Universidad".

Alulema, D. (2008), en su tesis: ''Estudio y diseño de un sistema de seguridad perimetral para la red Quito Motors" en la Escuela Politécnica Nacional - Ecuador. Concluye lo siguiente:

"Todos los mecanismos y consideraciones de seguridad en la red son necesarios para brindar una seguridad aceptable a una entidad, y mediante la tecnología UTM (Gestión Unificada de Amenazas) es posible establecer un nivel de seguridad coherente a las necesidades de empresas e instituciones, ya que permite cubrir los asuntos de seguridad más importantes.

Las soluciones de seguridad planteadas mediante el uso de dispositivos UTM (Gestión Unificada de Amenazas), ayudarán a proteger de manera más profunda los activos informáticos y el de los usuarios de la entidad; además permitirá brindar seguridad a las comunicaciones entre sucursales y con el Internet; también contribuirá en la implementación de aplicaciones seguras para el desarrollo de servicios web."

Valenzuela, J. (2012), en su tesis: "Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña", en la Pontificia Universidad Católica del Perú. Concluye lo siguiente:

“Antiguamente se pensaba que la seguridad de la información era un asunto meramente técnico que debía ser resuelto mediante la utilización de un componente tecnológico. Se creía incluso que el costo de este componente podía ser incluido dentro del presupuesto de otros departamentos, como por ejemplo, TI (Tecnología de la Información).

Hoy en día no es solo un aspecto tecnológico, muy por el contrario, es una solución integrada que combina estrategias, procesos y tecnología. Si no se cuenta con reglas, responsabilidades y procedimientos definidos, y con personal capacitado para la gestión de los procesos, la inversión en tecnología no es más que una pérdida de dinero.

La seguridad de la información debe lograr el equilibrio adecuado entre la protección y la habilitación de acceso a los activos de información. Debe enfocarse en proteger la información de la organización contra pérdidas o uso indebido de la misma.”

Yánez, C. (2008), en su tesis: “Diseño e implementación de plataforma de seguridad perimetral informática: Dirección Ejecutiva de la Magistratura” en la Universidad Simón Bolívar – Perú. Concluye lo siguiente:

“En estos tiempos de las telecomunicaciones, Internet, virus, hackers, software espía, spam, fraudes electrónicos, entre otros, es imprescindible la seguridad en redes, sistemas y aplicaciones. El enorme crecimiento de los sistemas de computación y sus interconexiones mediante redes ha hecho que organizaciones e individuos dependan cada vez más de la información que se almacena y transmite a través de estos sistemas, lo que ha conllevado a su vez

a un aumento de la conciencia sobre la necesidad de proteger los datos y los recursos, de garantizar la autenticidad de los datos y de los sistemas frente a ataques externos e internos, dentro de la red o desde Internet. Estas condiciones han generado paralelamente el desarrollo de aplicaciones, equipos y tecnologías para la prevención, detección de estos ataques y distintos riegos de seguridad que pueden afectar negativamente los datos, sistemas, aplicaciones, equipos e incluso operatividad de los mismos."

2.2. BASES TEÓRICAS

2.2.1 SEGURIDAD PERIMETRAL ADMINISTRADA (SPA)

La seguridad perimetral se basa principalmente en un firewall administrado con funciones avanzadas que le permitirán controlar y restringir todo lo que entra y sale de la red, proporcionando un gran control sobre lo que navegan los usuarios, ataques de hackers, virus y proporciona herramientas con túneles VPN (Red Privada Virtual) y reportes avanzados de tráfico de navegación web.

Algunas de las características de la solución son:

- Filtrado por origen y destino IP (Protocolo Internet), el protocolo IP (Protocolo Internet), puerto de origen y destino para el tráfico TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagramas de Usuario).
- Limitar conexiones simultáneas.
- Permite filtrar por el sistema operativo que inicia la conexión.

- Políticas de enrutamiento de alta flexibilidad que permite seleccionar diferentes puertas de enlace en alguna regla (Balanceo de Carga, Failover, Multi-Wan, etc)

- Permite gestionar múltiples WAN (Red de Área Amplia) permitiendo hacer balanceo de carga y Failover (Conmutación de errores).

- Ofrece 3 opciones para establecer túneles virtuales: VPN - PPTP (Red Priva Virtual – Protocolo de Túnel Punto a Punto), IP-Sec (Seguridad del Protocolo Internet) y Open VPN (Red Privada Virtual).

- Genera amplia información para evaluación de servicios como gráficas de uso de interfaces.

- Soporta DNS (Sistema de Nombres de Dominio) dinámico con gran cantidad de proveedores de este servicio.

En la figura 1, muestra los principales equipos que se deben contar para poder armar un diagrama de red segura en un perímetro local.

.

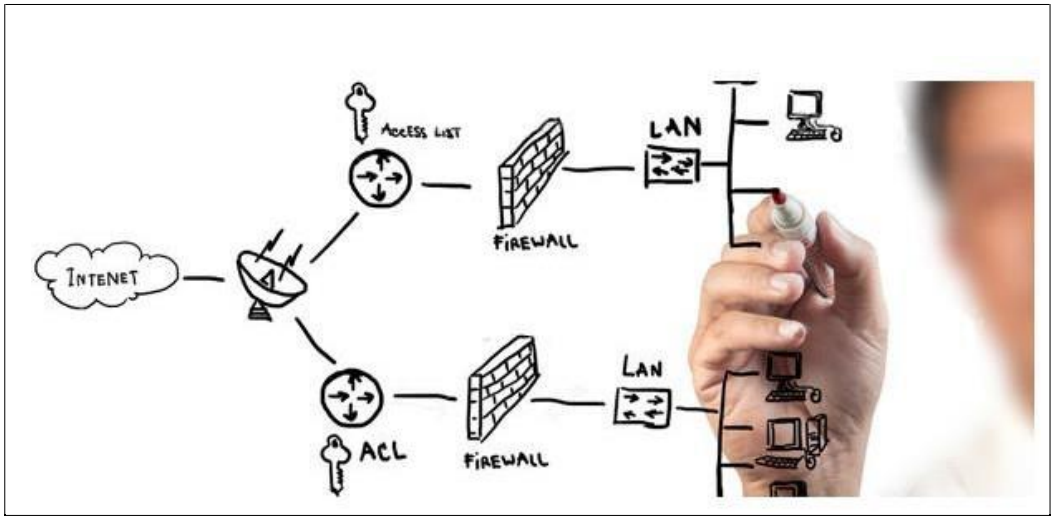


Figura 1: Red de Seguridad Perimetral

Fuente: http://www.catelca.com/seguridad.html

2.2.2. LAN (RED DE ÁREA LOCAL)

Una red local Ethernet es una red informática de área local o red LAN (Red de Área Local) que utiliza el protocolo Ethernet para la comunicación entre sus dispositivos interconectados por cables.

Una LAN (Red de Área Local) es un grupo de dispositivos interconectados que están bajo el mismo control administrativo. Las LAN (Red de Área Local) utilizan protocolos para comunicarse y el protocolo más frecuente en las redes locales conectadas por cable es Ethernet. Por lo tanto una red local Ethernet es una red local donde todos los hosts están conectados por cables y utilizan el protocolo Ethernet para comunicarse.

Ethernet es la tecnología LAN (Red de Área Local) más ampliamente utilizada en la actualidad. Ethernet es una familia de tecnologías de red que se definen en los estándares IEEE 802.2 y IEEE 802.3.

Las principales características con las siguientes:

- ✓ **Aspectos de Comunicación:** El protocolo Ethernet define los aspectos de la comunicación en una red local Ethernet. Esto incluye el formato y el tamaño de la trama, la temporización y la codificación.

- ✓ **Encapsulación de datos:** La encapsulación de datos incluye el armado de una trama por el emisor, antes de la transmisión y el desarmado de la trama por el receptor.

- ✓ **Formato de trama Ethernet:** La estructura de la trama de Ethernet agrega encabezados a la PDU (Unidad de Datos del Protocolo) de Capa 3 para encapsular el mensaje que se envía. El formato de una trama Ethernet incluye:

  El inicio de trama (preámbulo y delimitador de trama).

  - El direccionamiento
  - Los datos
  - La verificación de trama

- ✓ **Tamaño de trama Ethernet:** Se define el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes. Cualquier trama con menos de 64 bytes de longitud se considera un “fragmento de colisión” o “runt frame” y el host receptor la descarta.

- ✓ **Temporización del mensaje:** Para la sincronización entre el host emisor y el host receptor se utilizan delimitadores de tramas. Los

delimitadores de trama identifican un grupo específico de bits dentro de una trama. Estos bits van a captar la atención de los nodos receptores.

Ethernet usa la tecnología de acceso múltiple por detección de portadora (CSMA) para controlar la forma en que los hots (huésped) acceden al medio de comunicación. Con el método CSMA/Detección de colisión (CSMA/CD), el dispositivo detecta la presencia de datos en el medio. Si no hay datos, que indica que el medio está libre, el dispositivo transmite los datos. Si se detecta que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después. En toda comunicación es necesaria una forma de identificar el origen y el destino.

- ✓ **Direccionamiento de una red IP (Protocolo Internet):** En una red IP existen dos direcciones principales asignadas a un host, la dirección física (dirección MAC) y la dirección lógica (dirección IP).

La dirección MAC (Control de Acceso al Medio) y la dirección IP operan juntas para identificar un dispositivo en la red. Para que una computadora pueda comunicarse en una red, se necesitan tanto la dirección MAC (Control de Acceso al Medio) como la dirección IP (Protocolo Internet).

Cada nodo de una red IP tiene una dirección MAC (Control de Acceso al Medio) y una dirección IP. El nodo receptor utiliza sus propias direcciones MAC (Control de Acceso al Medio) e IP (Protocolo Internet) como el origen del mensaje y proporciona la dirección MAC

(Control de Acceso al Medio) y la dirección IP (Protocolo Internet) del nodo de destino.

- ✓ **Dirección física:** En una red local Ethernet cada dispositivo tiene que determinar si es el receptor previsto. Para identificar los dispositivos de origen y de destino reales dentro de una red Ethernet se utiliza la dirección física.

  Las direcciones físicas son únicas en el mundo y no cambian. La dirección física se asigna a cada interfaz de red Ethernet (NIC) en el momento de su fabricación. La dirección física es siempre la misma, independientemente del lugar en donde se encuentre el host (huésped).

  A la dirección física se le conoce como dirección de control de acceso al medio (MAC).

- ✓ **Dirección lógica**: Las direcciones lógicas cambian porque dependen del segmento de red donde se encuentra el host (huésped).

  La dirección lógica se asigna a cada host de forma lógica, por un administrador de red según la red local en la que el host está conectado. La dirección lógica también se puede asignar por medio de un servidor DHCP (Protocolo de configuración Huésped Dinámico).

  La dirección lógica se conoce como dirección IP o también como dirección de red.

- ✓ **Comunicación a través de una red local Ethernet:** Un host en una red local Ethernet se puede comunicar con otro host conectado en el mismo

segmento de red o se puede comunicar con otro host conectado en una red remota. Un host en una red local Ethernet puede acceder a recursos tanto locales como remotos.

- ✓ **Host en la misma red local:** Cuando un host accede a recursos locales, se comunica con otro host conectado en el mismo segmento de red, como se muestra en la figura 2. Durante esta comunicación utiliza la dirección MAC (Control de Acceso al Medio) del host de destino para entregar el mensaje.

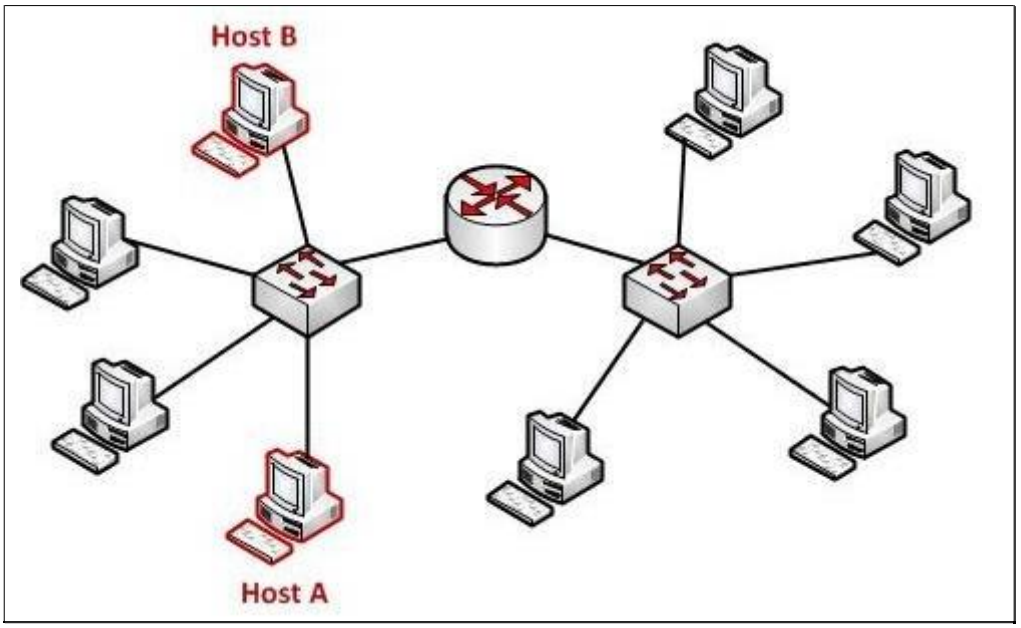


Figura 2:Comunicación de host locales

Fuente: http://www.osandnet.com/red-local-ethernet/

- ✓ **Host en una red remota;** Cuando un host accede a recursos remotos, como se muestra en la Figura 3, se comunica con otro host conectado en una red remota. Durante esta comunicación utiliza la dirección MAC (Control de Acceso al Medio) del gateway (puerta de enlace) predeterminado para entregar el mensaje al host de destino. [1]

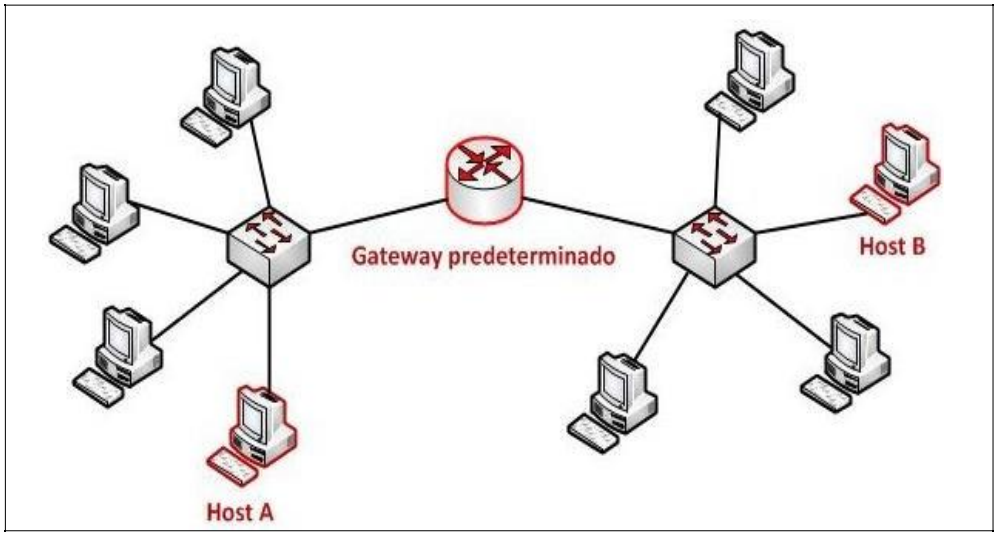


Figura 3: Comunicación de host en distinta redes locales

Fuente: http://www.osandnet.com/red-local-ethernet/

2.2.3 TECNOLOGÍA UTM (FIREWALL)

UTM viene de las siglas en ingles de: Unified Threat Management, o más bien Gestión Unificada de Amenazas. Entonces un Firewall UTM básicamente es un cortafuego de red que engloban múltiples funcionalidades (servicios) en una misma máquina de protección perimetral. Algunos de estos servicios son:

- Función de un firewall de inspección de paquetes de datos.
- Función de VPN (Red Privada Virtual), para hacer túneles o redes privadas.
- Antispam, para evitar los correos no deseados o spam.
- Antiphishing, evitar el robo de información.
- Filtrado de contenidos, para el bloqueo de sitios no permitidos mediante categorías (Contenido adulto, video/audio, redes sociales, virus, descargas, etc).

- Antivirus de perímetro, evitar la infección de virus informáticos en computadoras clientes y servidores.
- Sistema Detección de Intrusos (IDS).
- Sistema Prevención de Intrusos (IPS).

Estos firewall inspeccionan cada paquete de datos que va o viene de Internet (u otra red externa/interna) a nivel de capa de aplicación, y éste puede trabajar de dos modos:

2.2.3.1 Modos Proxy:

Un proxy es un ordenador que sirve de intermediario entre un navegador web e Internet, el proxy contribuye a la seguridad de la red.

Hacen uso de proxies para procesar y redirigir todo el tráfico interno. El firewall UTM (Gestión Unificada de Amenazas) hace de cliente y de servidor, y es el intermediario indirecto de las comunicaciones desde y hacia el internet (u otras redes).

2.2.3.2 Modo Transparente:

No redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones hardware pero es la mejor alternativa de UTM (Gestión Unificada de Amenazas).

2.3 MARCO CONCEPTUAL

2.3.1 FUNDAMENTOS TEÓRICOS DE SEGURIDAD EN REDES

Con el avance tecnológico experimentado en los últimos años, se han abierto nuevas formas de comprender al mundo, ya que la interconexión a diferentes redes y sistemas, permite la exploración de nuevos espacios fuera de los límites de una organización, lo cual conlleva al aparecimiento de nuevas amenazas inherentes a la expansión de una red aislada a una red compartida.

La seguridad de la información es un aspecto primordial en un sistema de red moderna, pero por ser considerado de forma errónea como un factor que no influye directamente en la productividad del sistema, no se proporciona la atención adecuada ni los recursos necesarios a esta labor.

Debido a que los datos constituyen recursos intangibles, el valor de los mismos gira en función de la importancia relativa que tienen para cada individuo, institución, empresa y entidad pertinente. Pero más allá del valor que alguien puede dar a la información, el problema real es el mal uso de la misma, ya que al exponerse a la red mundial puede ser interceptada o almacenada para realizar delitos informáticos y causar pérdidas económicas.

La inseguridad informática no se concentra solamente en el Internet, sino en toda forma de ataque electrónico como los accesos no autorizados, virus, falsificación y robo de información, violando las principales reglas de seguridad como lo es la integridad, privacidad y autenticidad.

A causa de los diferentes peligros a los que se exponen en la actualidad los sistemas informáticos, se considera necesario procedimientos que permitan el

buen uso de recursos y contenidos, para garantizar la continuidad de operación y la seguridad de la información.

La seguridad es algo que comienza y termina en las personas, las mismas que son un componente importante dentro de un sistema; por tal motivo es importante inculcar los conceptos, usos y costumbres del manejo adecuado de los recursos informáticos a los usuarios; sin embargo esto requiere tiempo y esfuerzo.

2.3.1.1 Seguridad Informática

Los sistemas de información y los datos almacenados son uno de los recursos más valiosos con los que puede contar cualquier organización. La necesidad imperante del flujo de información y el traslado de recursos de un sitio a otro hace que aparezcan vulnerabilidades que ponen en riesgo la seguridad de la infraestructura de comunicación y toda la información que contienen sus nodos. Proteger la información y los recursos tecnológicos informáticos es una tarea continua y de vital importancia que debe darse en la medida en que avanza la tecnología, ya que las técnicas empleadas por aquellos que usan dichos avances para fines delictivos aumentan y como resultado los atacantes son cada vez más numerosos, mejor organizados y con mejores capacidades. Las amenazas que se pueden presentar provienen tanto de agentes externos como de agentes internos, por eso es importante que toda organización que quiera tener una menor probabilidad de pérdida de recursos por causa de los ataques a los que se expone defina una estratificas que estén respaldadas por todos los miembros de la organización. [2]

Se debe considerar que la violación de la seguridad en un sistema podría llegar a afectar gravemente las operaciones más importantes de la empresa y dejarla expuesta a la quiebra.

En este sentido y considerando la alta volatilidad y especialidad de las vulnerabilidades, es necesario establecer programas de verificación y validación de las prácticas de seguridad informática con el fin de persuadir a los intrusos y valorar el estado del arte de esta función en la organización, es decir, ejercicios como pruebas de vulnerabilidades, auditorías de seguridad y evaluaciones de seguridad deben ser parte integral de la manera como la organización estima su nivel de riesgo real, frente a acciones intrusitas de terceros o internos sobre los sistemas de información.

Las tendencias en inseguridad informática son tan variantes como las relaciones que se presenten entre los diferentes elementos que la componente: tecnología, procesos o individuos, por tanto la única predicción válida en inseguridad de la información se concentra más que todo en algunas vulnerabilidades tecnológicas, otros en procedimientos (cuando se roban o pierden elementos de Sistemas tecnología) o en comportamientos no deseados de los individuos frente a la información y sus usos autorizados.

El futuro de la inseguridad exige de los profesionales de la seguridad un constante estudio de los riesgos y relaciones cambiantes del entorno de negocios para mantener una posición vigilante frente los movimientos de los intrusos, pues "a la hora que menos pensemos llega el ladrón y nos sorprende". En este sentido, es preciso diseñar y proponer sistemas de inteligencia informática para aprender sobre los indicadores ambientales y

tecnológicos que permitan visualizar cambios o vectores de ataques que mantengan nuestra motivación para continuar aprendiendo de la esencia misma de la protección de los activos: la inseguridad.

La seguridad de la información debe estar orientada a garantizar o mantener tres cualidades propias de esta última: disponibilidad, integridad y confidencialidad. En algunos entornos, especialmente en los dedicados a la Administración Electrónica, interesan, además, otros aspectos muy importantes de las transacciones on-line como son la autenticidad o la trazabilidad.

2.3.1.2 Amenazas

Es cualquier cosa que pueda alterar la operación, funcionalidad, integridad o disponibilidad de una red o sistema.

A) Formas de la Amenaza

- ✓ **Interrupción:** Provoca que un objeto del sistema se pierda, quede inutilizable o no disponible, su detección es inmediata.
- ✓ **Interceptación:** Cuando un elemento no autorizado consigue acceso a un elemento del sistema, su detección es difícil a veces no deja huellas.
- ✓ **Modificación:** Cuando a más de conseguir el acceso, consigue modificar un objeto del sistema con el fin de obtener beneficios. Se considera también como la destrucción del objeto si el mismo queda inutilizable.

- ✓ **Generación:** Cuando se crea o modifica un objeto con el fin de asemejarse a uno original, para pretender engañar al sistema, constituyen delitos de falsificación y su detección es difícil.

B) Tipos de Amenaza

- ✓ **Amenaza Pasiva:** Atenta contra la confidencialidad de la información sin cambiar el estado del sistema. Consiste en el acceso no autorizado a la información protegida, mediante la escucha o monitoreo con el fin de obtener la información transmitida y así averiguar o utilizar información del sistema, sin afectar los recursos del mismo.

- ✓ **Amenaza Activa:** Provoca un cambio no autorizado y deliberado del estado del sistema; intenta alterar los recursos del sistema o influir en su normal funcionamiento; busca modificar el flujo de datos o crear flujos falsos.

  Origen de las Amenazas:

  - Humanas
  - Personal
  - Ex empleados
  - Curiosos
  - Hackers

- ✓ **Amenazas Lógicas:** Constituyen todo tipo de programas que de una forma u otra pueden dañar un sistema, creados de forma intencional (software malicioso) o errónea (bugs).

  - Software incorrecto
  - Herramientas de seguridad
  - Malware

- ✓ **Amenazas Físicas:** Las catástrofes (naturales o artificiales) son la amenaza menos probable, sin embargo es importante tomar medidas básicas de protección, ya que si se produjeran generarían daños de gran impacto. Como ejemplos de catástrofes tenemos: terremotos, inundaciones, incendios, humo o atentados de baja magnitud.

  También existe un subgrupo de catástrofes con posibilidad de ocurrencia mínima, denominados riesgos poco probables, por lo tanto no vale la pena tomar medidas de seguridad contra éstas, ya que el sistema de prevención resultaría costoso e innecesario.

2.3.1.3 Vulnerabilidades

Es una debilidad inherente al diseño, configuración o implementación de una red o sistema, que lo deja susceptible a ataques.

A) Diseño pobre: Se presenta en los sistemas hardware y software que contienen fallas de diseño que pueden ser explotadas, es decir que el sistema ha sido creado con huecos de seguridad.

B) Implementación pobre: Se presenta en los sistemas configurados incorrectamente y por lo tanto son vulnerables a un ataque; estos tipos de vulnerabilidades son el resultado de desconocimiento, inexperiencia, entrenamiento insuficiente o descuido en el trabajo.

C) Administración pobre: Son el resultado de procedimientos inadecuados, controles y verificaciones insuficientes. Las medidas de seguridad no pueden operar en un vacío, necesitan ser documentadas y monitoreadas.

2.3.1.4 Mecanismo

La seguridad informática en las redes y sistemas requiere de un ciclo continuo de protección, detección y respuesta.

A) Mecanismos de Prevención: Consiste en cerrar las brechas de seguridad para aumentan la fiabilidad de un sistema durante su funcionamiento normal, previniendo la ocurrencia de violaciones a la seguridad

B) Mecanismos de autenticación e identificación: Permiten identificar entidades del sistema de una forma única para posteriormente autenticarlas (comprobar que la entidad es quien dice ser).

C) Mecanismos de control de acceso: Controlan todos los tipos de acceso sobre cada objeto por parte de cualquier entidad del sistema.

D) Mecanismos de separación: Se utilizan cuando un sistema maneja diferentes niveles de seguridad, para evitar el flujo de información entre objetos y entidades de diferentes niveles sin la exigencia de una autorización expresa del mecanismo de control de acceso. Tenemos mecanismos de separación física, temporal, lógica y criptográfica.

E) Mecanismos de seguridad en las comunicaciones: Se utilizan para garantizar la privacidad e integridad de los datos cuando se transmiten por la red. Algunos de estos mecanismos se basan en la criptografía como el cifrado de clave pública, de clave privada, firmas digitales, etc. Otros utilizan protocolos seguros como SSH (Secure SHell), Kerberos, etc. Los mecanismos de prevención se detallan más adelante en el subcapítulo Tecnologías de Seguridad Informática.

F) Mecanismos de Detección: Son aquellos que se utilizan para detectar violaciones a la seguridad o intentos de violación, ya que si no nos damos cuenta del ataque el daño va a ser mayor. Como ejemplo tenemos los programas de auditoría.

G) Mecanismos de Respuesta: Son aquellos que se aplican cuando una violación del sistema se ha detectado, ya que busca minimizar los efectos de un ataque o problema y finalmente retornar al sistema a su modo de trabajo normal. Como ejemplo tenemos las copias de seguridad o el hardware adicional (respaldos).

H) Mecanismo de análisis forense: Su objetivo es averiguar el alcance de la violación, las actividades del intruso en el sistema y la puerta utilizada para entrar; así se podrá prevenir ataques posteriores y detectar ataques a otros sistemas de nuestra red.

2.3.1.5 Modelos de Seguridad

A) Perímetro de defensa: Consiste en cercar la red o sistema a proteger, generalmente mediante un firewall que separe la red protegida de la red no confiable.

B) A nivel de red: Busca proteger al sistema informático de los ataques de hackers, intrusiones o robo de información en conexiones remotas.

C) A nivel de contenidos: Busca proteger al sistema de amenazas como los virus, gusanos, troyanos y demás clases de malware, del spam o correo basura y de los contenidos web no apropiados.

2.3.1.6 Seguridad en entidades

Las redes y sistemas pertenecientes a empresas teóricamente son las que representan mayores ventajas en lo relativo a su protección ya que suelen ser muy aislables.

Las empresas disponen de una red LAN (Red de Área Local) en el edificio donde están ubicadas, la misma que puede aislarse del exterior mediante un Firewall; pero si se ofrecen servicios hacia el exterior (correo electrónico y web), se pueden situar los servidores en una zona desmilitarizada entre el Router y la red interna. Además se tiene la conexión a Internet que brinda acceso hacia el exterior. Así la idealización de red aislada no sería posible con lo cual nos enfrentaríamos a los problemas de seguridad inherentes a esta apertura.

Las empresas cuentan con varias sucursales separadas geográficamente, para conectarlas tenemos dos opciones, hacerlo mediante una red propia (muy costoso) protegida por los técnicos de la misma compañía o mediante un

enlace arrendado a través de una red de propósito general como base de comunicaciones (red telefónica, Internet, etc.), así la protección de la red ya no depende exclusivamente de la propia organización, entonces es indispensable recurrir a VPN (Redes Privadas Virtuales), estableciendo canales de comunicación seguros dentro de redes inseguras.

El personal de las empresas cuenta con estaciones de trabajo móviles, las mismas que potencialmente pueden causar problemas de conectividad y seguridad, ya que una estación móvil puede entrar en contacto con ambientes inseguros y comprometer la información o infectarse, para seguidamente, introducirse en la organización y comprometer la seguridad de la misma.

Finalmente hay que considerar los ataques internos, que puede sufrir la organización por parte del personal propio de la empresa.

2.3.1.7 Políticas de Seguridad Informática

En la actualidad la gestión de la seguridad es algo crítico para cualquier organización, igual de importante que los sistemas de calidad o las líneas de producto que desarrolla.

Las políticas de seguridad son el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema, que indica lo que está y lo que no está permitido en el área de seguridad durante la operación general del sistema.

Sin una política de seguridad correctamente implantada en la organización no sirven de nada los controles de acceso (físicos y lógicos) implementados en la misma.

2.3.1.8 Políticas y Procedimientos

Las políticas y procedimientos de seguridad en una red o sistema sirven para asegurar la seguridad de la información, definen los niveles aceptables de seguridad de la información, mediante el planteamiento de aspectos como: ¿qué constituye la seguridad de la información?, ¿por qué es importante? y ¿cómo mantenerla? Para determinar el nivel de seguridad adecuado para cierta organización, se debe considerar los elementos de seguridad de la información: confidencialidad, integridad, disponibilidad, autenticación y control de acceso, de acuerdo a los requerimientos de la organización.

I. **Políticas de seguridad:** Son el conjunto de reglas y procedimientos que regulan cómo una organización administra, usa, protege y distribuye toda la información que directa o indirectamente le pertenece. Las políticas deben estar orientadas a qué posesiones proteger y por qué necesitan ser protegidos, son amplias en su alcance y son diseñadas para fijar el tono y la dirección. Son documentos que exhiben el ¿qué? Y ¿por qué? de la seguridad de la información para una organización, además deben ser simples de entender y fáciles de recordar.

II. **Procedimientos de seguridad:** El desarrollo de los procedimientos debe fluir desde las políticas de seguridad, estos deben ser más precisos y detallados, centrarse en las medidas específicas necesarias para proteger las posesiones de la organización. Son documentos que contienen el ¿quién?, ¿cuándo? Y ¿cómo? de la seguridad de la información dentro de una organización.

2.3.1.9 Técnicas de Ataques y Protecciones

Amenazas y ataques

A) Virus: Son una sección oculta y auto-replicable de software, por lo general con una lógica maliciosa, que se propaga mediante la infección, es decir, la inserción de una copia de sí mismo y convertirse en parte de otro programa. Un virus no se puede ejecutar por sí mismo, sino que requiere que su programa anfitrión sea ejecutado para lograr que el virus se active.

B) Worms – Gusanos: Es un programa de computador que puede funcionar de forma independiente, puede propagar una versión funcional completa de sí mismo en otras máquinas en una red, y puede consumir recursos del computador destructivamente.

C) Caballo De Troya: Son aquellos programas de computador que parecen tener una función útil, pero también poseen una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces mediante la explotación de autorizaciones legítimas de una entidad sistema que invoca el programa.

D) Ataque de Repetición: Consiste en interceptar y almacenar una transmisión legítima entre dos sistemas y retransmitirla un tiempo después.

E) Sniffing: Consiste en monitorear los paquetes de una red en busca de información (contraseñas o direcciones IP) que pueda ser útil para un ataque; también el análisis de tráfico puede proveer información útil. [3]

F) Modificación de Sitios Web: Consiste en modificar los sitios web de alguna organización, se consigue mediante la explotación de configuraciones

incorrectas y/o vulnerabilidades conocidas del software o sistema operativo del servidor Web. Para contrarrestar este ataque hay que actualizar las versiones del software y sistema operativo del servidor Web o implementar servidores caché de red que actualicen al servidor Web.

G) Negación del Servicio: Son diseñados para apagar o presentar inoperable un sistema, el objetivo es hacer a una red o sistema no disponible.

2.3.1.10 Protecciones

I. Secure Sockets Layer (SSL)

Fue desarrollado para brindar seguridad en la transmisión de información por Internet, ofrece confidencialidad al momento de ingresar o trasmitir datos por la Web. Se utiliza la encriptación asimétrica para preparar la sesión (Capa de Conexión Segura) y la encriptación simétrica para transmitir datos de forma segura sobre una red insegura.

II. HTTPS (Protocolo de Transferencia de Hipertexto Seguro)

Consiste en usar el servicio HTTP (Protocolo de Transferencia de Hipertexto) sobre SSL (Capa de Conexión Segura), SSL establece una conexión segura mediante el uso de un túnel encriptado entre el cliente browser (navegador) y el servidor Web, así los paquetes de datos viajan seguros. La integridad de la información se establece mediante algoritmos hash, la confidencialidad de la información es asegurada mediante la encriptación, la autenticación de las entidades se asegura mediante el uso de certificados digitales y encriptación asimétrica.

III. Seguridad E-Mail

Consiste en no revelar el contenido del mensaje e-mail mediante el uso de encriptación; asegurar la integridad del mensaje mediante el empleo de algoritmos hashing o message digest; verificar la identidad del transmisor mediante el empleo de firmas digitales y finalmente verificar la identidad del receptor mediante el uso de encriptación de clave pública.

2.3.1.11 Tecnologías de Seguridad Informática

I. FIREWALL

Es un sistema o dispositivo de control de acceso que se utiliza para separar una red interna de una red externa, se encuentra en el límite entre el espacio protegido denominado perímetro de seguridad y la red externa denominada zona de riesgo, filtra tráfico de entrada y salida, y también esconde la configuración de la red hacia el exterior.

La función del firewall, por tanto, es bloquear el tráfico no autorizado entre un sistema de confianza y un sistema de dudosa confianza.

Un firewall es, a menudo, instalado en el punto donde una red interna se conecta con Internet. Todo tráfico externo de Internet hacia la red interna pasa a través del firewall, así puede determinar si dicho tráfico es aceptable de acuerdo a sus políticas de seguridad.

Aunque el propósito principal de los firewall es mantener a los intrusos fuera del alcance de la información que es propiedad de un ente determinado, ya sea un usuario, una empresa o un gobierno, su posición dentro del acceso a distintas redes le vuelve muy útil para controlar estadísticas de situaciones

como usuarios que intentaron conectarse y no lo consiguieron, tráfico que atravesó la misma, etc... Esto proporciona un sistema muy cómodo de auditar la red. Algunas de sus funciones son las siguientes:

- Restringir la entrada a usuarios a puntos cuidadosamente controlados.
- Prevenir los ataques
- Dividir una red en zonas con distintas necesidades de seguridad.
- Auditar el acceso a la red.

I.a. Características de un Firewall

Un firewall, debido a su funcionalidad, debe ser capaz de ofrecer una serie de características mínimas como puede ser el empleo de una adecuada política de seguridad.

Por consiguiente, esto sólo no basta, sino que el firewall además debe de ser capaz de poder ofrecer otros servicios como pueden ser el registro de las operaciones que vaya realizando y el poseer una interfaz fácil e intuitiva que reduzca al mínimo la posibilidad de que el operario se equivoque a la hora de configurarlo y mantenerlo. Algunas de las características que definen a un firewall son:

I.b. Política de Seguridad

Consiste en determinar los principios generales en los que debe basarse el diseño de un sistema de seguridad, en nuestro caso un firewall:

- Política Principal: Todo aquello que no está expresamente permitido está prohibido.

- Política de Escepticismo: Tras dotar al firewall de todas las protecciones disponibles se toma en consideración que se pueden desarrollar nuevas técnicas y que ningún grado de seguridad es absoluto.

I.c. Registro de Operaciones

El firewall podía ser utilizado para obtener datos estadísticos acerca de la afluencia entre ambas redes. Pues bien, para poder realizar esta estadística deberá recoger, como mínimo, la siguiente información y almacenarla en algún fichero:

- Service Information - fecha y hora.

- Remote Information - dirección IP del presunto intruso, así como el puerto y el protocolo utilizado.

- Local Information - dirección IP de destino y puerto.

- Packet Information - encabezamiento e información del paquete.

Esta información también es muy útil en caso de producirse un ataque para poder conocer por donde se ha intentado entrar, cuándo y porqué, cuál ha sido la estrategia que ha seguido el firewall, si el ataque ha sido o no exitoso. Estos datos nos van a permitir poder hacer un seguimiento sobre el funcionamiento del firewall.

I.d. Interfaces

Con una política de seguridad lo suficientemente hermética y un firewall eficaz, el mayor riesgo provendrá de un error humano del administrador del firewall. Estos pueden incorporar un gran número de funciones que complican su trabajo de administración. Los firewall que cuentan con una buena interfaz reducen la posibilidad de errores humanos y simplifican el trabajo del administrador del firewall.

Una interfaz fácil de utilizar y con un número mínimo de opciones de configuración reduce la posibilidad de que se produzcan errores de administración. Naturalmente, un número menor de opciones de configuración puede significar también menor flexibilidad de configuración.

Existen tres clases de interfaz del administrador de firewalls:

- ✓ Administración basada en ficheros de texto.
- ✓ Administración basada en menús de texto.
- ✓ Administración basada en GUI (Interfaz Gráfica de Usuario)

La interfaz basada en ficheros de texto es la de uso más extendido en lo que respecta a los firewalls de elaboración propia. Este tipo de interfaces permiten al administrador editar un archivo específico donde puede introducir parámetros de configuración específicos. Se trata de la interfaz de elección para los administradores de sistemas UNIX tradicionales, dado que ofrece una interfaz de control a bajo nivel con los mecanismos del firewall. La desventaja de dicho control a bajo nivel es que resulta mucho más fácil cometer errores, ya

que, al editar un fichero, pueden producirse errores de escritura u otros errores técnicos que, en un sistema basado en menús, es menos probable que ocurran.

La interfaz de administrador basada en menús de texto presenta un menú basado en texto que reduce la probabilidad de producirse errores pero que proporciona menor capacidad de control para el administrador. Sin embargo, la posibilidad de error no queda totalmente excluida, dado que el administrador no siempre puede ver el efecto de algunos cambios.

La interfaz gráfica de usuario, o GUI, para administradores incorpora ventanas, botones, menús desplegables y pantallas de ayuda que facilitan el trabajo de configuración. La mayoría de proveedores ha optado por incluir esta interfaz en sus productos, puesto que tiende a ser más fácil de utilizar y no es susceptible a muchos de los errores que pueden producirse en los otros dos tipos de interfaz.

I.e. Autenticación de Usuarios

La dirección IP (Protocolo Internet) del host origen se emplea para efectuar el control básico de acceso. Sin embargo, esta dirección puede ser suplantada fácilmente, especialmente por hosts que forman parte de la misma red. Además, en el caso de conexiones procedentes de hosts multiusuario, la dirección de éstos no permite distinguir un usuario de otro. La mayoría de firewalls a nivel de aplicación soportan la autenticación de usuarios para algunos servicios de red. Para ello, el firewall interrumpe la conexión y solicita a

los usuarios que se identifiquen antes de continuar la conexión hacia el destino deseado.

Sin embargo, la mayoría de protocolos de servicio de red no toleran dicha interrupción y, por lo tanto, no pueden soportar los métodos de autenticación, como contraseñas y tarjetas inteligentes. Otros protocolos como el correo electrónico o los grupos de noticias no establecen una conexión directa con el usuario, por lo que no es posible solicitar información para la identificación.

Los servicios de red estándar que contemplan la posibilidad de que un firewall pueda realizar funciones de autenticación son Telnet y FTP (Protocolo de Transferencia de Archivos).

Los mecanismos estándar de autenticación que ofrecen los firewalls en la actualidad son contraseñas convencionales, tarjetas inteligentes y servicios S/Key. El mecanismo de contraseñas convencional emplea contraseñas multiuso y no es recomendable utilizarlo en Internet porque las contraseñas pueden ser interceptadas y empleadas más adelante por un intruso. Las tarjetas inteligentes verifican la identidad de un usuario devolviendo una respuesta única basada en un número aleatorio, que proporciona el firewall. Los usuarios responden introduciendo el número en un dispositivo autentificador, que calcula la respuesta apropiada.

I.f. Restricciones de Día y Hora

La política de seguridad puede variar en función de del día de la semana y la hora del día. Por ejemplo, es posible permitir transferir archivos a Internet durante las horas laborales normales, aunque no durante los fines de semana o

después de las 6 de la tarde. Algunos firewall permiten basar las reglas de acceso o listas de acceso en la hora del día y el día de la semana.

I.g. Control de la Carga

El control de la carga es una característica que ofrecen muy pocos firewalls. Para la mayoría de estos, cuando se permite el acceso, el host o la red pueden efectuar un número ilimitado de conexiones. Es útil poder establecer limitaciones al número de conexiones simultáneas con un host o una red de hosts que puede haber activas. Esta característica puede ayudar a impedir ataques por inundación, mediante los cuales un pirata informático inunda la red con conexiones a fin de ocultar el ataque real.

I.h. Canalización

La canalización es la capacidad de combinar múltiples servicios de aplicación en una única conexión. Los intrusos emplean en ocasiones esta técnica para disfrazar un servicio no autorizado (por ejemplo, FTP) como servicio autorizado (como el correo electrónico).

Un firewall puede proporcionar también la característica de canalización para permitir a dos sitios de una compañía compartir servicios en Internet que no serían autorizados normalmente a través del mismo.

I.i. Servidor Proxy

El proxy es una solución software que se ejecuta sobre el Firewall para permitir la comunicación entre dos redes de una forma controlada.

Proxy a nivel de aplicación. Son aplicaciones software (servicios proxy) para bloquear o reenviar conexiones a servicios como telnet, HTTP (Protocolo de Transferencia de Hipertexto), SMTP (Protocolo de Transferencia de Correo Simple) o FTP (Protocolo de Transferencia de Archivos); la máquina donde corren estas aplicaciones se denomina pasarela de aplicación. [4]

Los servicios proxy permiten únicamente la utilización de servicios para los que existe un proxy, además entiende el protocolo para el que fue diseñado lo que hace posible mayor capacidad de análisis y restricción; pero esto puede ser costoso, limitar el ancho de banda efectivo de la red o disminuir la funcionalidad de aplicaciones.

La pasarela de aplicación permite un grado de ocultación de la estructura de la red protegida, ya que es el único sistema que se presenta hacia el exterior, todas las conexiones se originan y terminan en las interfaces del Firewall.

2.3.1.12 VPN (Red Privada Virtual)

Es una red de datos privada creada a partir de una red de datos pública como Internet, transporta tráfico de una manera segura sobre una red insegura, mediante el uso de encriptación, autenticación y encapsulamiento (tunneling), con el fin de asegurar la integridad y privacidad de los datos. Existen varias razones para la implantación de VPNs (Redes Privadas Virtuales):

- Bajo costo de implementación.
- Privacidad de los datos.
- Acceso desde todas partes.

- Flexibilidad.

- Escalabilidad.

I. Seguridad

A) Privacidad de los datos

- Modo Encriptación. Consiste en cifrar la porción de datos del paquete usando encriptación simétrica o asimétrica, la cabecera del paquete no es modificada.

- Modo Túnel. Todo el paquete de datos incluida la cabecera es encapsulado dentro de un nuevo paquete el mismo que es encriptado y finalmente se le añade una nueva cabecera, este modo es usado para transmitir protocolos no IP sobre el backbone IP o IP dentro de IP por razones de seguridad. [5]

- Integridad de los datos. Para asegurar la integridad de los datos las soluciones VPN (Red Privada Virtual) utilizan los algoritmos hash.

- Autenticación. Las soluciones VPN (Red Privada Virtual) soportan varios esquemas de autenticación de usuarios como: Usuario / Contraseña.

B) Autenticación vía token: Smartcards, Certificados X.509.

C) Autorización. Las soluciones VPN (Red Privada Virtual) permiten definir perfiles de usuario con su correspondiente nivel de autorización y acceso.

D) Control de acceso. Las soluciones VPN (Red Privada Virtual) proveen un control de acceso por razones de seguridad y auditoría basado en:

• User ID.

• Host ID.

• IP address.

• Subnetwork address.

E) Auditoría. Las soluciones VPN (Red Privada Virtual) definen un registro de actividad del usuario.

F) Rendimiento. El tiempo de respuesta entre una red segura y una red insegura deben ser semejantes, para brindar transparencia a la solución VPN, el trabajo adicional que acarrea el uso de VPNs (Redes Privadas Virtuales) incrementa la latencia y disminuye la velocidad efectiva de los datos.

Entonces es importante considerar los siguientes parámetros al comprar o diseñar una solución VPN (Red Privada Virtual):

• Calidad de servicio (QOS).

• Acuerdos de nivel de servicio (SLAs).

• Soporte de múltiples protocolos.

• Confiabilidad y resistencia.

2.3.1.13 Modelos de Autenticación

Los sistemas de una organización deben tener la capacidad de restringir el acceso a sus diferentes recursos dependiendo de la identificación y autorización que posee el usuario.

A) Contraseñas: Cualidad que el individuo conoce, las contraseñas brindan una seguridad débil ya que una contraseña puede ser adivinada, robada u obtenida.

B) Tarjetas inteligentes: Cualidad que el individuo tiene, las tarjetas inteligentes proporcionan una seguridad mayor pero no completa, evitan el riesgo de que una contraseña sea descubierta, pero si una tarjeta es robada y constituye el único medio de autenticación una atacante explotará esta vulnerabilidad del sistema para tener acceso al mismo.

C) Software Antimalware: Son programas que escanean los virus, son muy efectivos contra virus conocidos, pero son incapaces de reconocer y adaptarse a nuevos virus.

Su funcionamiento radica en el reconocimiento de la firma de un virus conocido, el programa detecta un virus cuando encuentra una coincidencia entre los resultados escaneados y las firmas de virus almacenadas en la base de datos. La base de datos que contiene las firmas de virus debe ser actualizada regularmente caso contrario el programa antivirus se vuelve obsoleto rápidamente.

Constituye un componente necesario para una buena solución de seguridad, ya que si está implementado y configurado apropiadamente, puede reducir la exposición de una organización a programas mal intencionados.

Sin embargo no protegerá a una organización de un intruso que haga mal uso de un programa legítimo para obtener el acceso al sistema, tampoco si un usuario legítimo intenta obtener acceso a archivos a los que no tiene acceso.

2.3.1.14 Sistemas de Detección de Intrusos (IDS)

Constituyen sistemas administradores competentes que auditan y monitorean continuamente sus sistemas en busca de intrusiones. La detección de intrusiones es el arte de detectar actividades no autorizadas, inapropiadas o extrañas.

Los IDS (Sistema de Detección de Intrusos) son capaces de detectar ataques en progreso, generar alarmas en tiempo real y contrarrestar un ataque mediante el lanzamiento de un evento o la reconfiguración del router o Firewall.

Actúan como guardianes de seguridad o centinelas, constantemente están escaneando el tráfico de red o los logs (eventos) de auditoría de un host.

2.3.1.15 Sistemas de Detección de Intrusos para Host (HIDS)

Reside en el host y es capaz de monitorear y negar servicios automáticamente si una actividad sospechosa es detectada; usan los archivos log y los agentes de auditoría del sistema para realizar el monitoreo.

A) Verificadores de Integridad del Sistema (SIV). Es un mecanismo encargado de monitorizar archivos de una máquina en busca de posibles modificaciones no autorizadas.

B) Monitores de Registros (LFM). Monitorizan los archivos de log generados por los programas de una máquina en busca de patrones que puedan indicar un ataque o una intrusión.

C) Sistemas de decepción. Son mecanismos encargados de simular servicios con problemas de seguridad de forma que un pirata piense que realmente el

problema se puede aprovechar para acceder a un sistema, cuando realmente se está aprovechando para registrar todas sus actividades.

2.1.3.16 Sistemas de Detección de Intrusos para Red (NIDS)

Monitoriza los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella; el IDS (Sistema de Detección de Intrusos) puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico (como un HUB o un enrutador); éste analiza los siguientes elementos:

- ✓ Campos de fragmentación IP (Protocolo Internet).
- ✓ Dirección origen y destino.
- ✓ Puerto origen y destino.
- ✓ Campo de datos.

2.1.3.17 Detección de Anomalías

La base del funcionamiento de estos sistemas es suponer que una intrusión se puede ver como una anomalía de nuestro sistema, estos modelos de detección conocen lo que es normal en nuestra red o nuestras máquinas a lo largo del tiempo, desarrollando y actualizando conjuntos de patrones contra los que se compararán los eventos que se producen en los sistemas, se tiene:

- Métodos estadísticos que determinan los perfiles de comportamiento habitual.
- Especificación de reglas que establecen los perfiles de comportamiento normal.

2.1.3.18 Detección de Usos Indebidos

El funcionamiento de los IDS (Sistema de Detección de Intrusos) basados en la detección de usos indebidos presupone que podemos establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones, este esquema se limita a conocer lo anormal para poder detectar intrusiones, se tiene:

- ✓ Sistemas expertos.
- ✓ Transición de estados.
- ✓ Comparación y emparejamiento de patrones.
- ✓ Detección basada en modelos.

2.3.1.19 Seguridad Física de Red

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y detección contra las amenazas a los recursos y a la información confidencial. Éste suele ser un aspecto olvidado frecuentemente, lo cual motiva a los atacantes a explotar las vulnerabilidades físicas del sistema.

Entonces implementar cierta seguridad física es importante para garantizar la seguridad global de la red y los sistemas conectados a ella; pues se podría implementar un sistema sofisticado de seguridad lógica pero no serviría de nada si un intruso accede físicamente al sistema u ocurre una catástrofe que puede causar mucho más daño que una amenaza lógica.

Para establecer un sistema de seguridad física se ha de analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado.

I. Protección del Hardware

Las medidas encaminadas a asegurar la integridad del hardware son parte importante de la seguridad física de cualquier organización, ya que frecuentemente constituye el componente más caro de todo sistema informático.

II. Acceso Físico

Comprende la protección de zonas o elementos físicos que pueden comprometer la seguridad del sistema, es así que el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger, ya que se tendrán equipos bien protegidos dentro de la organización y otros ubicados en lugares de acceso casi público. La posibilidad de acceder físicamente a un sistema hace inútiles casi todas las medidas de seguridad que se hayan aplicado.

- Prevención. Consiste en implementar mecanismos de control de acceso, para prevenir un ingreso físico no autorizado. Los más adecuados para la seguridad física son los biométricos y los basados en algo que el individuo posee, así entre los más comunes tenemos videocámaras, geometría de la mano, huellas digitales, tarjetas inteligentes, control de las llaves que abren determinada puerta.

- Detección. Consiste en implementar mecanismos que permitan conocer la presencia de accesos no autorizados, entre los más comunes tenemos cámaras de vigilancia, alarmas o personal de la organización.

III. Protección de los datos

La seguridad física también implica una protección a la información del sistema, tanto a la que está almacenada como a la que se transmite entre diferentes equipos.

• Interceptación. Es un proceso mediante el cual un agente capta información (plana o cifrada) que no le pertenece. Mediante el sniffing un atacante puede capturar tramas que circulan por la red, para contrarrestar esta amenaza hay que evitar tener segmentos de red de fácil acceso o tomas de red libres y usar aplicaciones de cifrado para las comunicaciones o almacenamiento de la información (hardware de cifrado).

También puede filtrarse la información (reuniones) mediante teléfonos fijos o móviles, para evitar esto se pueden desconectar los teléfonos fijos y bloquear la señal de los móviles mediante un sistema de aislamiento que bloquea cualquier transmisión en los rangos de frecuencias en los que trabajan las operadoras telefónicas.

• Backups. Consiste en la protección de los diferentes medios donde residen las copias de seguridad, ya que contienen toda la información, hay que protegerlas igual que a los sistemas en sí; se puede realizar backups cifrados y controlar más el acceso al lugar donde se guardan.

2.3.1.20 UTM (Unified Threat Management)

I. Estudio de la tecnología UTM (Gestión Unificada de Amenazas)

Los avances de la tecnología y el desarrollo de amenazas cada vez más peligrosas y complejas, ha determinado que las soluciones de seguridad perimetral evolucionen a los sistemas de seguridad multi-amenazas, que constituyen la nueva generación de los sistemas de protección de red en tiempo real.

Los sistemas unificados de administración de amenazas (UTM) detectan y eliminan las más dañinas amenazas basadas en el contenido e-mail o tráfico web tales como virus, gusanos, intrusiones, contenido web inapropiado y más en tiempo real, sin degradar el rendimiento de la red.

En la Figura 4, se muestran los principales equipos a proteger con el protocolo UTM (Gestión Unificada de Amenazas).

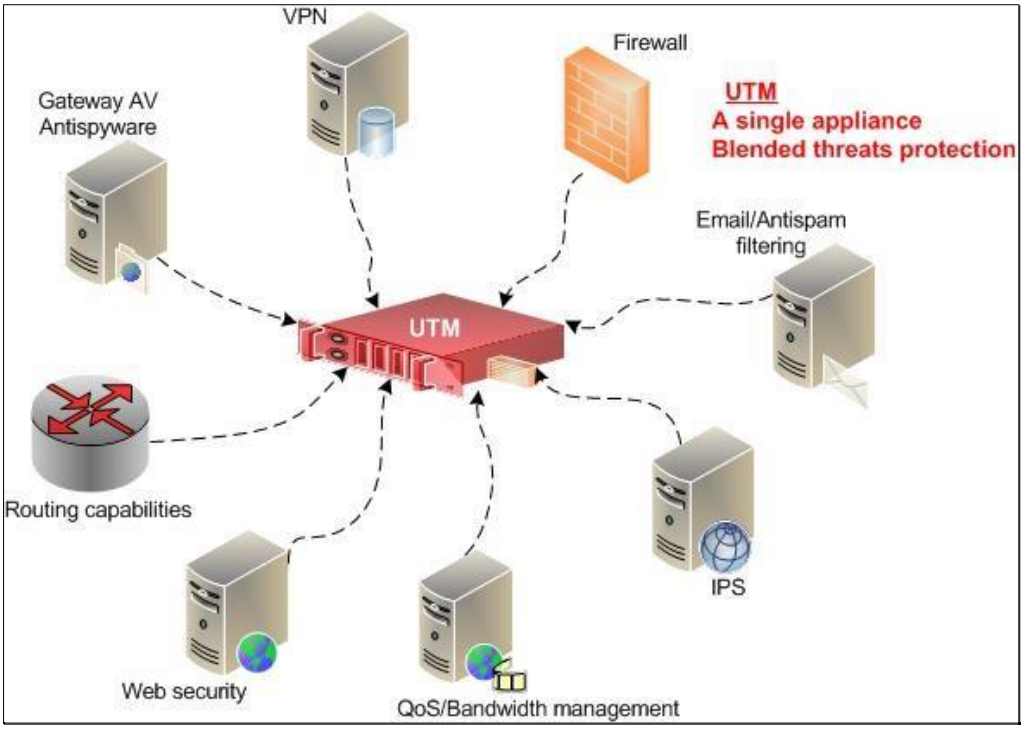


Figura 4: Gestión Unificada de Amenazas

Fuente: http://www.firewalls.com/what_is_utm_firewall

Un sistema de seguridad debe poseer varios componentes que trabajen conjuntamente con el fin de aproximarse a un sistema seguro, es así, que los sistemas UTM incorporan varias técnicas y componentes de seguridad para lograr el acercamiento a este objetivo.

Los sistemas reinantes actualmente como los Firewall, VPNs (Redes Privadas Virtuales) e IDS (Sistema de Detección de Intrusos) resultan efectivos proporcionando protección a nivel de red, sin embargo no cubren las necesidades de protección actual en los ámbitos telemáticos, ya que su capacidad permite el análisis de la cabecera de los paquetes pero no el análisis del contenido de los mismos.

Estos sistemas no pueden comprobar el contenido del paquete y procesarlo para identificar virus, gusanos u otras amenazas, por lo tanto son ineficaces contra ataques basados en contenido. Así los virus, gusanos, troyanos, etc, transmitidos por correo electrónico y tráfico http atraviesan fácilmente los Firewall, VPN (Red Privada Virtual) o IDS (Sistema de Detección de Intrusos).

Toda esta evolución de tecnología ha acelerado la necesidad de implantación de soluciones de defensa en profundidad a nivel de contenido. Aparentemente el reto de los fabricantes y proveedores de seguridad es la gestión eficiente de respuesta ante los nuevos ataques que nacen en el Internet y en proporcionar firmas actualizadas y efectivas para controlar dichos ataques.

Los sistemas UTM (Gestión Unificada de Amenazas) constituyen el software y hardware específico para la seguridad de redes, sus más comunes y principales características son el uso de tecnología ASIC (Application-Specific-Integrated Circuit) y la integración de diferentes módulos de seguridad que garantizan la adecuada protección de la red sin degradar su rendimiento. [6]

Finalmente para complementar la seguridad en entornos extremadamente críticos se incluye HIDS (Sistema de detección de intrusos en un Host), sistemas de seguridad en profundidad encargados de detectar y proteger a un sistema en particular de intrusiones; así se puede controlar de manera exhaustiva los datos, aplicaciones y accesos que se procesan en una determinada máquina.

Los dispositivos UTM (Gestión Unificada de Amenazas) combinan las funciones de diferentes dispositivos de seguridad, administración y análisis dentro de un solo ambiente más flexible lo cual permite desarrollar en forma integral múltiples características de seguridad (políticas de seguridad) en una sola plataforma.

Estos sistemas están ganando popularidad rápidamente debido al rendimiento que ofrecen en aplicaciones de seguridad, costo de operación e inversión de capital.

2.3.2 Análisis Solución de Implementación: FortiGate de Fortinet

En el mercado existen muchas soluciones UTM como lo son las ofrecidas por los fabricantes Fortinet, SonicWall, Check Point Software Technologies, Watchguard, Juniper, Cisco, Netgear, entre otros. El análisis de la solución UTM FORTIGATE del fabricante FORTINET, para el caso puntual de la Universidad Nacional de Trujillo, entidad en la que se desarrolla el presente proyecto, obedece a que esta es la solución que han implementado otras instituciones del grupo al que pertenece esta entidad y la institución la ha tomado como solución estándar, para todas sus sedes. A pesar de esta limitante en la selección de un UTM (Gestión Unificada de Amenazas), se realiza un análisis del comparativo del Cuadrante mágico para UTM (Gestión Unificada de Amenazas) realizado por la entidad Gartner en Mayo del 2016, como se muestra en la Figura 5.

Figura 5: Cuadrante mágico para UTMs realizados por la entidad Gartner

Fuente:https://www.tecnozero.com/blog/gartner-2016-para-los-firewalls-de-redes-empresariales/

En la Figura 5, se detalla que la entidad Gartner sitúa la solución UTM (Gestión Unificada de Amenazas) de FORTINET cómo líder en el mercado, con la mayor habilidad de ejecución y visión completa frente a las funcionalidades que ofrece las soluciones UTM (Gestión Unificada de Amenazas), a diferencia de otras soluciones del mercado.

A continuación se detallan las fortalezas y debilidades, de acuerdo a los lineamientos de la entidad Gartner en el informe Magic Quadrant for Unified Threat Management respecto a la solución UTM Fortinet:

2.3.2.1 FORTALEZAS

- ✓ Fortinet se presenta en la mayoría de listas de candidatos y sigue innovando. En el mercado de medianas empresas, se considera una "opción segura", debido a su fuerte presencia en este mercado.
- ✓ El uso de Fortinet de hardware a la medida, combinada con precios agresivos, sigue ofreciendo un alto nivel de precio / rendimiento.
- ✓ Tiene aplicación flexible y fácil de conocer las capacidades políticas de firewall, estrechamente vinculada a las políticas de IPS.

2.3.2.2 DEBILIDADES:

- ✓ Fortinet IPS es difícil de ajustar con precisión.
- ✓ La falta de pruebas de rendimiento independientes dificulta la capacidad de los compradores más avanzados para verificar las afirmaciones acerca de su rendimiento.
- ✓ Las funciones de registros y presentación de informes del dispositivo son muy básicas.

Por otro lado Fortinet ofrece una completa gama de productos (software y hardware), servicios de subscripción y soporte que trabajan conjuntamente para proporcionar soluciones de seguridad de red amplias, rentables y manejables; cuenta además con certificaciones FIPS (Federal Information

Processing Standards) e ICSA (International Computer Security Association) y características NSS (Network Security Services) y EAL (Evaluation Assurance Level).

Los sistemas de seguridad multi-amenaza de Fortinet utilizan tecnología ASIC (Application-Specific Integrated Circuit) y constituyen la nueva generación de protección de red en tiempo real; detectan y eliminan las amenazas más perjudiciales de correo electrónico y tráfico web sin degradar el rendimiento de la red. Las tecnologías que se usan para estos tipos de sistema de seguridad son como las que se muestran en la Figura 6. [7]

Figura 6: Principales Tecnologías y ámbitos del Fortinet

Fuente: https://www.fortinet.com/

2.3.2.3 Fortiguard Distribution Network (FDN)

Es una red mundial de servidores FortiGuard distribuidos que permite actualizar las definiciones de ataques. La infraestructura FortiGuard de Fortinet asegura la rápida identificación de nuevas amenazas y el desarrollo de firmas de nuevos ataques. Los servicios de FortiGuard constituyen un valioso recurso para el cliente e incluye actualizaciones automáticas de virus, motores IPS y definiciones a través de la FDN.

2.3.2.4 FortiGuard Center

Presenta la base de datos de vulnerabilidades y amenazas, la misma que es mantenida y actualizada por el equipo mundial de respuesta de amenazas de Fortinet y provee cobertura de 24x7x365 sobre las más recientes amenazas globales.

Estos servicios son creados con la más reciente tecnología de seguridad y diseñados para operar con el menor costo. Con la subscripción de servicios FortiGuard habilitada, los clientes pueden estar seguros que seguros que sus plataformas de seguridad FortiGate están funcionando óptimamente y protegiendo sus activos corporativos con la última tecnología de seguridad y con el mejor precio posible.

A) Servicio Antivirus FortiGuard: Proporciona protección automática para el Firewall Antivirus de FortiGate y lo mantiene actualizado con las últimas defensas antivirus contra amenazas basadas en red.

B) Servicio IPS FortiGuard: Proporciona a los clientes FortiGate las últimas defensas contra actividades de red maliciosas, sospechosas o secretas,

provenientes de nuevas y desconocidas amenazas y vulnerabilidades mediante las cuales se pretende ganar acceso a la red, a sus aplicaciones importantes o a la información; este servicio toma medidas de precaución y responde a los ataques que se propagan rápidamente en la actualidad.

C) Servicio de Filtrado Web FortiGuard. Regula y proporciona una valiosa comprensión de las actividades web, permitiendo a los clientes satisfacer las nuevas regulaciones gubernamentales, cumplimiento educacional, políticas de recursos humanos y políticas de uso de Internet corporativo; así previene el uso inapropiado de Internet que provoca bajas en la productividad, utilización inadecuada de los recursos empresariales, hostigamiento, deuda legal y demás cuestiones de recurso humanos.

Como se muestra en la Figura 7, son las principales característica de análisis para el control de transferencia de datos.

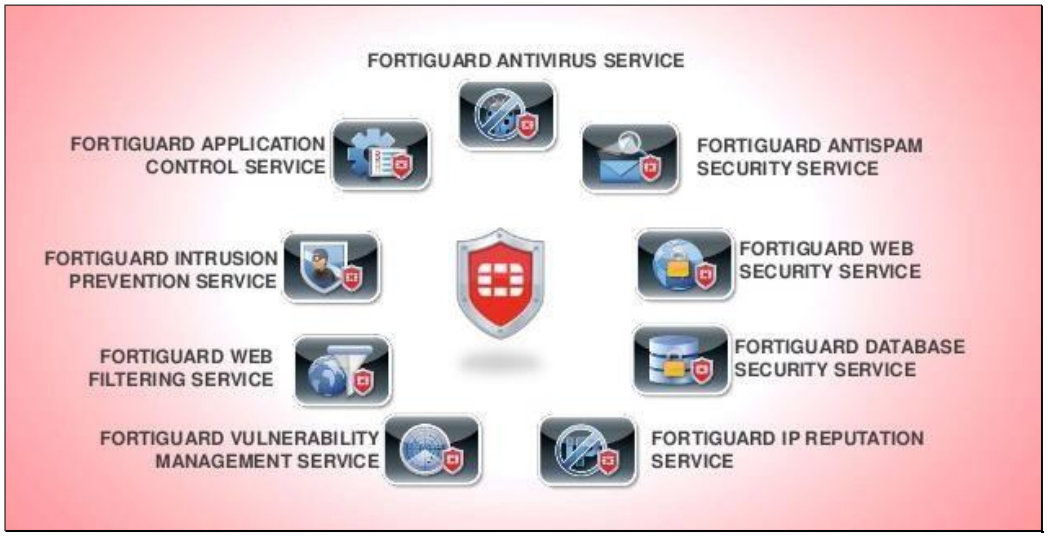


Figura 7: Servicio FortiGuard

Fuente: https://fortiguard.com/

2.3.2.5 FortiGate

Es un sistema de administración de amenazas unificado (UTM) que mejora la seguridad de red, reduce el mal uso y abuso de la red y ayuda a utilizar más eficientemente los recursos de comunicaciones sin comprometer el rendimiento de la red. Los sistemas UTM FortiGate cuentan con certificaciones ICSA para firewall, IPSec y Antivirus. [8]

FortiGate es un dispositivo de seguridad dedicado y de fácil administración que ofrece un paquete completo de capacidades entre las cuales se incluye:

- ✓ Servicios a nivel de aplicación. Ofrecen protección contra virus y filtrado de contenido.
- ✓ Servicios a nivel de red. Ofrecen protección mediante firewall, detección / prevención de intrusiones, VPN y modelado de tráfico.

El sistema UTM FortiGate utiliza tecnología DTPS (Dynamic Threat Prevention System), que aprovecha los avances tecnológicos en:

- Diseño del chip.
- Red.
- Seguridad.
- Análisis de contenido.

La arquitectura basada en tecnología ASIC (Application-Specific Integrated Circuit) analiza el contenido y el comportamiento en tiempo real lo que permite

que aplicaciones de seguridad claves sean desplegadas justo en el límite de red donde son más eficaces para la protección de la misma.

I. Estado del Sistema

A) Página de Estado. Expone información del sistema, información de licencias, recursos del sistema, consola CLI (Interfaz de Línea de Comando), estado de la interfaz, consola de mensajes de alerta, estadística de tráfico y protección.

B) Información del Sistema. Permite cambiar la hora, el nombre y el modo de operación para el VDOM (Dominio Virtual).

C) Firmware FortiGate. Permite actualizar a una nueva versión o regresar a una versión antigua del software FortiOS.

D) Historial de operación. Permite visualizar seis gráficos que presentan los recursos del sistema y la actividad de protección.

E) Definiciones FortiGuard. Permite actualizar las bases de datos de las diferentes herramientas FortiGuard:

- Antivirus.
- Prevención de Intrusiones.
- AntiSpam.
- AntiSpyware.
- Visor de estadísticas. Muestra información sobre sesiones, archivos de contenido y actividad de protección de red.

- Visor de Topología. Permite diagramar y documentar las redes conectadas a la unidad FortiGate, para establecer un control y monitoreo de las mismas.

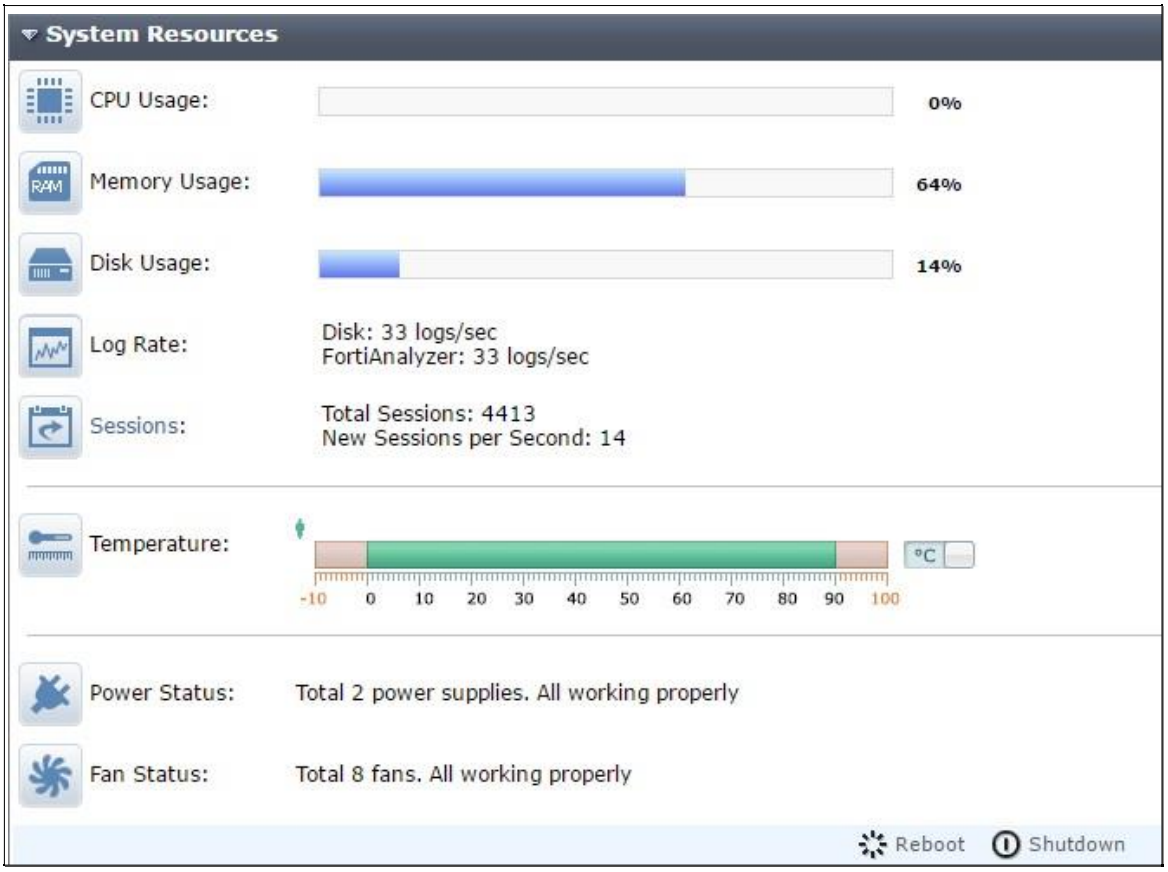


Figura 8: Estado del sistema en el FortiGate

Fuente: Elaboración propia

II. Uso de Dominios Virtuales

Los dominios virtuales (VDOMs) permiten a la unidad FortiGate funcionar como múltiples unidades virtuales independientes; una sola unidad puede servir separadamente a varias redes y ser la base de la administración del servicio de seguridad.

Los VDOMs (Dominios Virtuales) proporcionan diferentes dominios de seguridad que permiten separar zonas, autenticar usuarios, aplicar políticas de firewall / ruteo y configurar VPNs (Redes Privadas Virtuales). Por defecto cada unidad tiene un VDOM (Dominio Virtual) llamado root, que incluye todas las interfaces físicas, sub interfaces VLAN (Red de Área Local Virtual), zonas, políticas de firewall, configuraciones router y VPN (Red Privada Virtual). [9]

III. Configuración FortiGate

A) Modo NAT / Router

En este modo la unidad FortiGate es visible para la red, sus interfaces están en diferente subred. Se puede establecer políticas de firewall para controlar las comunicaciones a través de la unidad FortiGate que controla el tráfico basado en la dirección origen, dirección destino y servicio de cada paquete.

En la Figura 9, se muestra las sedes remotas la cual deben tener acceso hacia la red central de la universidad, para ello se realizara el modo NAT, para la comunicaciones entre sedes.

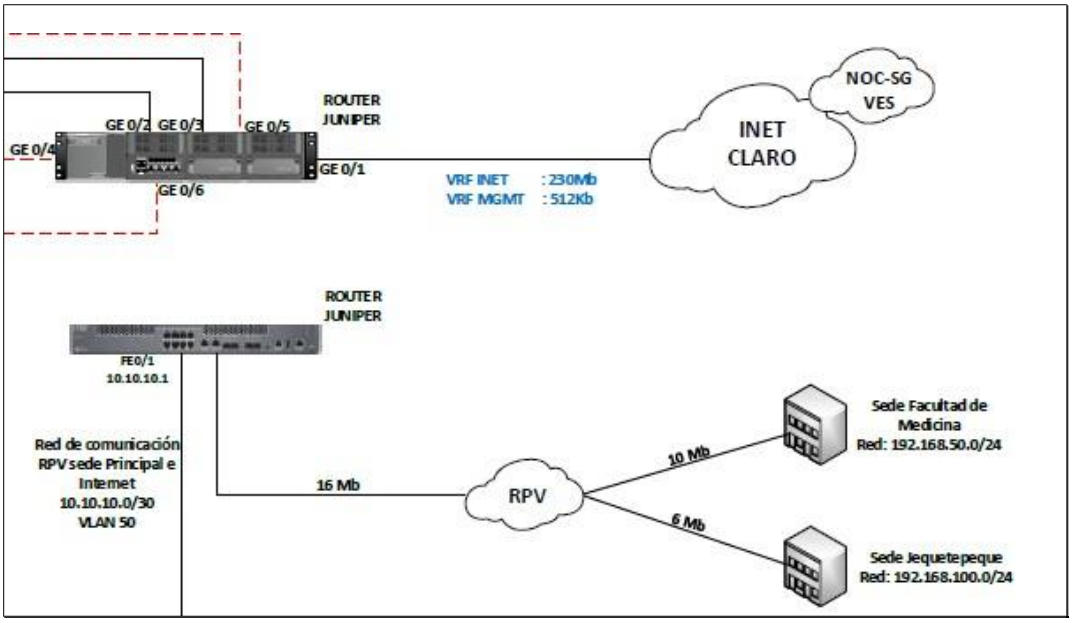


Figura 9: Configuración Modo NAT / Router.

Fuente: Elaboración propia

En el modo NAT FortiGate realiza la traducción de la dirección de red antes de enviar el paquete a la red destino; en el modo Router no hay traducción de dirección. Se usa el modo NAT/Router cuando la unidad FortiGate está operando como un Gateway entre las redes pública y privada, se crean políticas de firewall en modo NAT para controlar el tráfico entre la red interna y la red externa y políticas de firewall en modo router para controlar el tráfico entre las redes internas.

B) Modo Transparente

En el modo transparente la unidad FortiGate no es visible para la red, su comportamiento es similar a un puente de red y todas las interfaces de la unidad deben estar en la misma subred; solamente se configura una dirección IP de administración para poder realizar cambios en la configuración, actualizar el antivirus y las amenazas.

El modo transparente se usa en redes privadas detrás de un firewall existente o detrás de un router.

La unidad FortiGate realiza las funciones de firewall, IPSec VPN, escaneo de virus, filtrado web, IPS y filtrado Spam; pueden conectarse hasta doce segmentos de red a la unidad FortiGate para controlar el tráfico de red entre éstos.

2.3.2.6 Administración del Sistema

Existen dos niveles de cuentas de administradores:

A) Administrador Regular. Es asignado a una VDOM (Dominio Virtual) y no puede tener acceso a la configuración global o a la configuración de otro VDOM (Dominio Virtual) al cual no haya sido asignado.

B) Administrador de Sistema. Tiene acceso completo a la configuración de la unidad FortiGate.

I. Perfil de acceso

Cada cuenta de administrador pertenece a un perfil de acceso; el perfil de acceso separa en categorías el control de acceso a las características de la unidad FortiGate, se puede habilitar accesos de lectura y/o escritura.

II. Mantenimiento del sistema

Se puede respaldar la configuración del sistema, incluyendo los archivos de contenido web y archivos de filtrado spam a la computadora que administra o a un disco usb; también se puede restaurar la configuración del sistema de archivos de respaldo descargados con anterioridad.

III. Centro FortiGuard

El centro FortiGuard configura a la unidad FortiGate para acceder a la red de distribución FortiGuard (FDN) y a los servicios FortiGuard.

La red de distribución FortiGuard proporciona actualización de antivirus, definiciones de ataques, lista negra de direcciones IP en línea, lista negra de URL y otras herramientas de filtrado spam.

La lista negra de direcciones IP contiene direcciones IP de servidores e-mail que se conoce son usados para generar spam.

La lista negra de URL contiene URLs de sitios web encontrados en e-mails spam; también proporciona cientos de millones de páginas web clasificadas en un amplio rango de categorías que el usuario puede permitir, bloquear o monitorear.

IV. Ruteo Estático

Una ruta proporciona a la unidad FortiGate la información necesaria para enviar un paquete a un destino particular en la red; una ruta estática hace que los paquetes se envíen a un destino diferente del configurado por defecto. Opcionalmente se pueden definir políticas de ruteo, que permiten especificar criterios adicionales para examinar las propiedades de los paquetes entrantes, mediante el uso de políticas de ruteo se puede configurar a la unidad FortiGate para que dirija paquetes basándose en la dirección IP de origen y/o destino, la interfaz por la cual el paquete fue recibido, el protocolo (servicio) y/o el puerto que está siendo usado para transportar el paquete.

V. Ruteo dinámico

Trabaja con protocolos dinámicos para enrutar el tráfico a través de redes grandes y complejas; los protocolos dinámicos habilitan a la unidad FortiGate para que comparta información de ruteo automáticamente con routers vecinos y aprenda sobre rutas y redes anunciadas por sus routers vecinos. La unidad FortiGate soporta los siguientes protocolos de enrutamiento dinámico:

- ✓ Routing Information Protocol (RIP).
- ✓ Open Shortest Path First (OSPF).
- ✓ Border Gateway Protocol (BGP).
- ✓ Protocol Independet Multicast (PIM).

VI. Políticas Firewall

Las políticas firewall controlan todo el tráfico que pasa a través de la unidad FortiGate, son instrucciones usadas para decidir qué hacer con una petición de conexión.

Cuando el Firewall recibe una petición de conexión en forma de paquete, éste es analizado para extraer la dirección origen, la dirección destino y el servicio (número de puerto), para ser evaluado con las políticas de firewall y tomar acciones sobre el paquete, como permitir la conexión, negar la conexión, pedir autenticación antes de permitir la conexión o procesar al paquete como un paquete VPN IPSec (Red Privada Virtual – Protocolo de Internet Seguro).

VII. Virtual IP – Firewall

A) Virtual IPs: Las direcciones IP virtuales pueden ser usadas para permitir conexiones a través de la unidad FortiGate usando políticas firewall de tipo NAT (Traducción de Direcciones de Red).

Las IPs virtuales usan un proxy ARP (Protocolo de Resolución de Dirección) para que la unidad FortiGate pueda responder a peticiones ARP (Protocolo de Resolución de Dirección) pertenecientes a un servidor que actualmente está instalado en otra red; así la unidad FortiGate se presenta como el servidor y la red interna permanece oculta al público.

B) Pool de IPs: Son utilizadas para añadir políticas NAT (Traducción de Direcciones de Red) que traduzcan dinámicamente direcciones origen de los paquetes salientes a direcciones aleatorias seleccionadas del pool IP antes que limitarse a la dirección IP de la interfaz de destino. Un pool IP define una dirección o un rango de direcciones IP que responden a las peticiones ARP (Protocolo de Resolución de Dirección) en la interfaz a la cual ha sido asignado el pool IP. [10]

C) Perfil de protección Firewall: El perfil de protección es un grupo de configuraciones que pueden modificarse para ajustarse a un propósito particular; se pueden usar perfiles de protección para cada tipo de tráfico que maneja una política firewall, se tiene:

- Configurar la protección antivirus para políticas HTTP (Protocolo de Transferencia de HyperTexto), FTP (Protocolo de Transferencia de Archivos), IMAP (Protocolo de Acceso a Mensajes de Internet), POP3

(Protocolo de Oficina de Postal), SMTP (Protocolo de Transferencia Simple de Correo) e IM (Mensajería Instantánea).

- Configurar el filtrado web para políticas HTTP (Protocolo de Transferencia de HyperTexto) y HTTPS (Protocolo de Transferencia de HyperTexto Seguro).
- Configurar el filtrado web por categorías para políticas HTTP (Protocolo de Transferencia de HyperTexto) y HTTPS (Protocolo de Transferencia de HyperTexto Seguro).
- Configurar el filtrado spam para políticas (Protocolo de Acceso a Mensajes de Internet), POP3 (Protocolo de Oficina de Postal) y SMTP (Protocolo de Transferencia Simple de Correo).
- Habilitar IPS (Sistema de Prevención de Intrusos) para todos los servicios.
- Configurar el archivo de contenido para políticas HTTP (Protocolo de Transferencia de HyperTexto), FTP (Protocolo de Transferencia de Archivos), IMAP (Protocolo de Acceso a Mensajes de Internet), POP3 (Protocolo de Oficina de Postal), SMTP (Protocolo de Transferencia Simple de Correo) e IM (Mensajería Instantánea). [11]
- Configurar filtrado IM y control de acceso para mensajería instantánea AIM, ICQ, MSN, Yahoo y SIMPLE.

- Configurar acceso P2P y control del ancho de banda para clientes punto a punto BitTorrent, eDonkey, Gnutella, Kazaa, Skype, WinNY, Emule y Ares.

- Configurar cuales acciones del perfil de protección serán registradas.

- Mediante los perfiles de protección se puede personalizar los tipos y niveles de protección para diferentes políticas firewall.

La unidad FortiGate tiene pre-configurados cuatro perfiles de protección:

- Estricto: Aplica máxima protección al tráfico HTTP (Protocolo de Transferencia de HyperTexto), FTP (Protocolo de Transferencia de Archivos), IMAP (Protocolo de Acceso a Mensajes de Internet), POP3 (Protocolo de Oficina de Postal), SMTP (Protocolo de Transferencia Simple de Correo).

- Escanear: Aplica escaneo de virus al tráfico HTTP (Protocolo de Transferencia de HyperTexto), FTP (Protocolo de Transferencia de Archivos), IMAP (Protocolo de Acceso a Mensajes de Internet), POP3 (Protocolo de Oficina de Postal), SMTP (Protocolo de Transferencia Simple de Correo).

- Web: Aplica escaneo de virus y bloqueo de contenido web para el tráfico HTTP (Protocolo de Transferencia de HyperTexto).

- No filtrado, no aplica escaneo, bloqueo o IPS (Sistema de Prevención de Intrusos).

VIII. IPSec (Internet Protocol Security)

La unidad FortiGate implementa el protocolo ESP (Encapsulated Security Payload), donde los paquetes encriptados aparecen como paquetes ordinarios que pueden ser enrutados a través de cualquier red IP, el procedimiento IKE (Internet Key Exchange) es realizado automáticamente basándose en pre-shared keys o certificados digitales X.509, aunque también se pueden especificar claves manualmente. [12]

Cuando se define una ruta basada en un túnel IPSec (Protocolo de Internet Seguro), una interfaz IPSec virtual es creada automáticamente como una sub-interfaz en la interfaz física, agregada o VLAN (Red de Área Local Virtual) de la unidad FortiGate esto es conocido como IPSec (Protocolo de Internet Seguro) modo interfaz.

Una interfaz virtual IPSec (Protocolo de Internet Seguro) es considerada en funcionamiento cuando puede establecer una conexión de Fase 1 con un punto similar VPN (Red Privada Virtual) o un cliente; sin embargo la interfaz virtual IPSec (Protocolo de Internet Seguro) no puede ser usada para enviar tráfico a través de un túnel hasta pasar a la Fase 2 de definición; después de que una interfaz virtual IPSec ha sido asignada a un túnel, el tráfico puede ser enrutado a la interfaz usando métricas específicas tanto para rutas estáticas como para políticas de rutas, además se pueden crear políticas de firewall considerando a la interfaz virtual IPSec (Protocolo de Internet Seguro) como la interfaz origen o destino.

Cuando el tráfico IP (Protocolo Internet) se origina detrás de la unidad FortiGate local busca una interfaz FortiGate de salida que actúe como el punto final local del túnel IPSec (Protocolo de Internet Seguro), el tráfico es encapsulado por el túnel y enviado a través de la interfaz física a la cual pertenece la interfaz virtual IPSec (Protocolo de Internet Seguro).

Cuando el tráfico encapsulado de un punto VPN (Red Privada Virtual) remoto o de un cliente busca una interfaz física local de la unidad FortiGate, ésta determina si una interfaz virtual IPSec está asociada a la interfaz física a través de selectores en el tráfico; si el tráfico coincide con los selectores predefinidos, éste es des-encapsulado y enviado a la interfaz virtual IPSec (Protocolo de Internet Seguro).

En la dirección saliente, la unidad FortiGate realiza un lazo de ruteo para encontrar la interfaz a través de la cual debe enviar el tráfico para alcanzar el siguiente router, si la unidad encuentra una ruta a través de una interfaz virtual que está ligada a un túnel VPN (Red Privada Virtual) específico, el tráfico es encriptado y enviado a través del túnel VPN (Red Privada Virtual).

En la dirección entrante, la unidad identifica un túnel VPN (Red Privada Virtual) usando la dirección IP de destino y el SPI (Security Parameter Index) en el datagrama ESP, luego para completar la Fase 2 se analiza la SA (Security Association); si una coincidencia SA es encontrada, el datagrama es des encriptado y el tráfico IP asociado es re direccionado a través de la interfaz virtual IPSec.

Fase 1. Como se muestra en la Figura 10, en la Fase 1 los dos puntos VPN (Red Privada Virtual) se autentican uno al otro e intercambian claves para establecer un canal de comunicación segura entre ellos.

- ✓ Intercambio de información de autenticación encriptado o no encriptado.
- ✓ Uso de pre-shared key o certificados digitales para la autenticación de las entidades de los puntos VPN (Red Privada Virtual).
- ✓ Uso de un identificador especial, un certificado de nombre distinguido o nombre de grupo para identificar el punto VPN (Red Privada Virtual) remoto o cliente remoto.

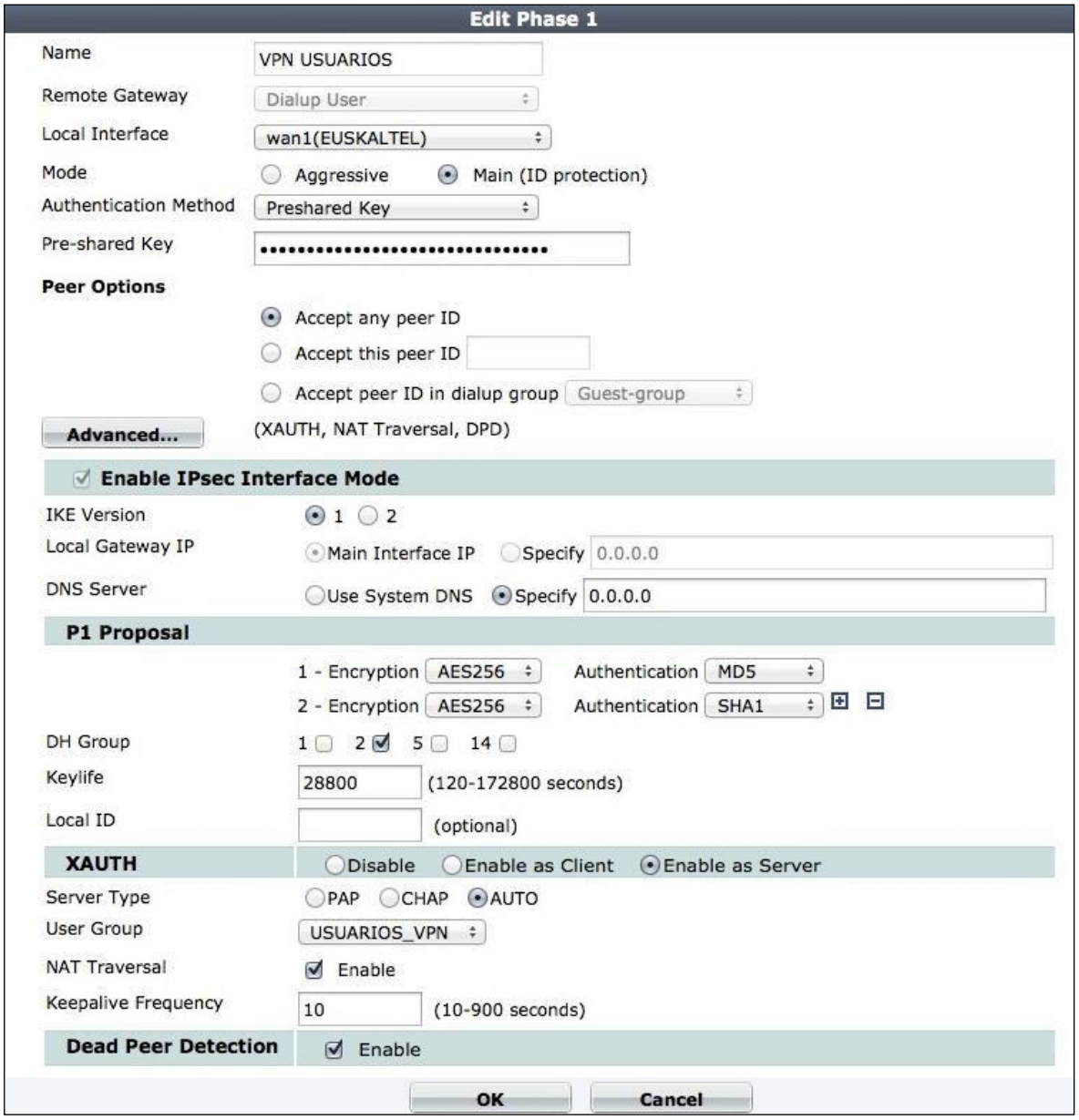


Figura 10: Fase 1 – VPN IPSec

Fuente: Elaboración propia

Fase 2. Como se muestra en la Figura 11, los parámetros de la Fase 2 definen los algoritmos que la unidad FortiGate puede usar para cifrar y transferir los datos por el resto de la sesión; durante la Fase 2, las asociaciones de seguridad específicas de IPSec (Protocolo de Internet Seguro) requeridas para implementar servicios de seguridad son seleccionadas y un túnel es establecido.

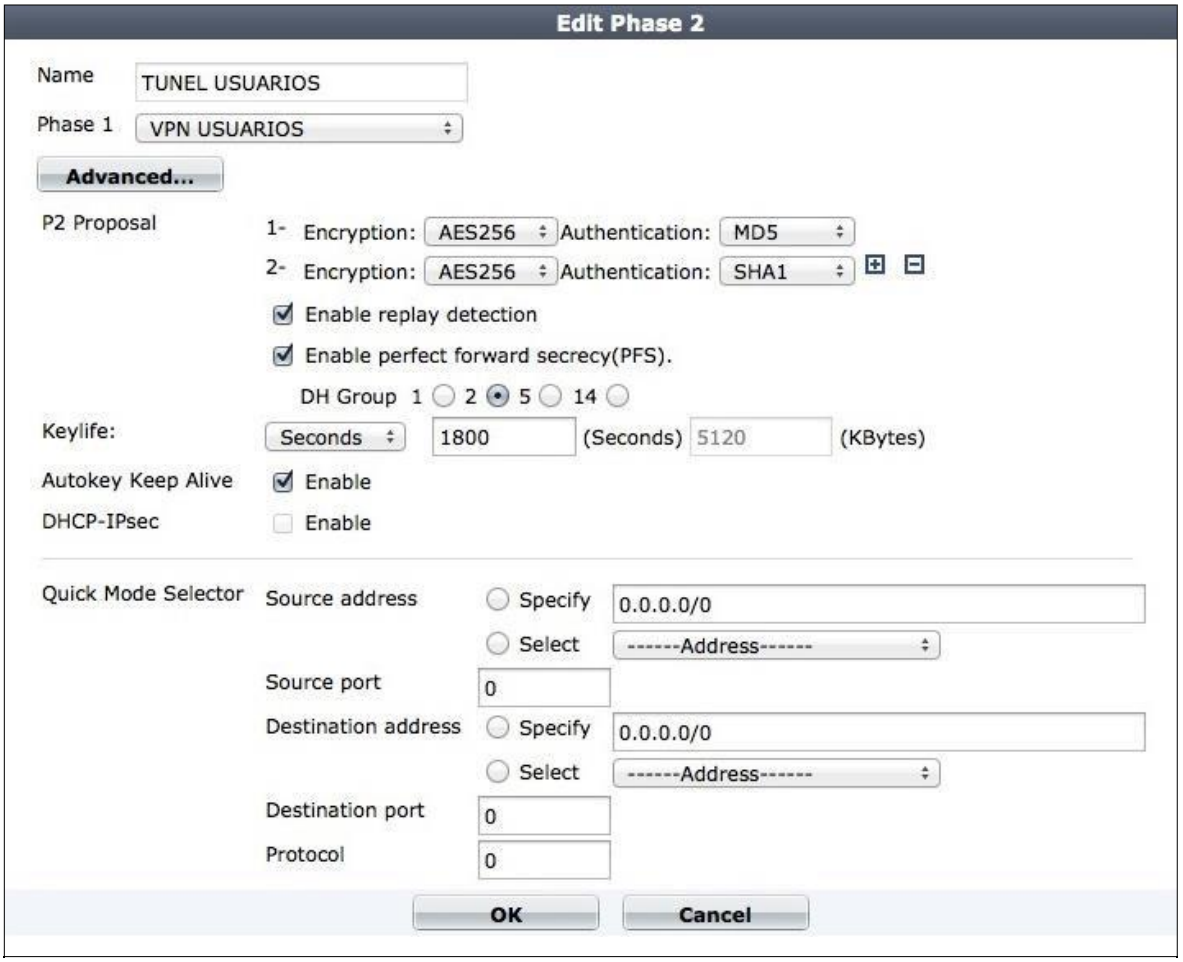


Figura 11: Fase 2 – VPN IPSec

Fuente: Elaboración propia

IX. Autenticación de Usuarios

A) Servidor RADIUS: Si el usuario requiere autenticarse usando un servidor RADIUS, la unidad FortiGate envía las credenciales del usuario al servidor RADIUS para su autenticación; si el servidor RADIUS puede autentificar al usuario, el mismo es autentificado exitosamente con la unidad FortiGate, caso contrario la conexión es rechazada por la unidad FortiGate.

B) Servidor LDAP (Protocolo Compacto de Acceso a Directorios): Si el usuario requiere autenticarse usando un servidor LDAP (Protocolo Compacto de Acceso a Directorios), la unidad FortiGate contacta al servidor LDAP (Protocolo Compacto de Acceso a Directorios) para la autenticación. Para autenticarse con la unidad FortiGate el usuario ingresa un nombre y contraseña, los mismos que son enviados al servidor LDAP (Protocolo Compacto de Acceso a Directorios), donde se realiza el procedimiento de autenticación, si el usuario es autenticado positivamente obtiene el accesos a la unidad FortiGate, caso contrario la conexión es rechazada. Adicionalmente FortiGate LDAP soporta LDAP sobre SSL/TLS.

C) Autenticación PKI: Utiliza una biblioteca de certificados de autenticación, así los usuarios necesitan solamente un certificado válido para su autenticación.

D) Servidor AD (Directorio Activo) de Windows: En las redes que usan servidores Windows Active Directory (AD) para la autenticación, la unidad FortiGate puede autenticar a los usuarios de forma transparente sin necesidad de preguntarles su nombre de usuario y contraseña, para lo cual se debe instalar FSAE (Fortinet Server Authentication Extensions) en la red y configurar la unidad FortiGate para recuperar información del servidor Windows AD (Directorio Activo).

X. Grupo de Usuario

Es una lista de identidades de usuario, donde una identidad puede ser:

- ✓ Una cuenta de usuario local (nombre de usuario y contraseña) almacenado en la unidad FortiGate.
- ✓ Una cuenta de usuario local con una contraseña almacenada en un servidor
- ✓ RADIUS o LDAP (Protocolo Compacto de Acceso a Directorios).
- ✓ Un servidor RADIUS o LDAP (Protocolo Compacto de Acceso a Directorios), todas las identidades almacenadas en el servidor pueden ser autentificadas.
- ✓ Un grupo de usuarios definidos en un servidor Microsoft Active Directory.

En la mayoría de los casos la unidad FortiGate autentica a los usuarios mediante su nombre de usuario y contraseña, primero chequea las cuentas de usuarios locales, luego los servidores RADIUS o LDAP (Protocolo Compacto de Acceso a Directorios) que pertenecen al grupo de usuario; la autenticación es exitosa cuando encuentra una coincidencia. Para el grupo de usuario de AD (Directorio Activo) la autenticación se realiza cuando el usuario entra a la red mediante el agente de FSAE la unidad FortiGate recibe el nombre de usuario y la dirección IP.

XI. AntiVirus

El procedimiento antivirus engloba varios módulos y motores que realizan tareas separadas; los elementos antivirus trabajan en secuencia para proporcionar un método de escaneo eficiente para los archivos entrantes; estos elementos trabajan para ofrecer a la red una protección antivirus incomparable.

Además para asegurar la mejor protección disponible, todas las definiciones y firmas de virus son actualizadas regularmente mediante los servicios antivirus FortiGuard.

XII. Archivo patrón

Una vez que un archivo es aceptado, la unidad FortiGate aplica el filtro de reconocimiento de patrón de archivo y compara el archivo entrante con el patrón de archivo configurado, si el archivo tiene un patrón de bloqueo, éste es detenido y un mensaje de reemplazo es enviado al usuario final, además ningún otro nivel de protección es aplicado; pero si el archivo no es bloqueado entonces otros niveles de protección son aplicados.

El patrón de archivos sirve para bloquear archivos que constituyen una potencial amenaza y prevenir los ataques de virus; los archivos pueden ser bloqueados por nombre, extensión o cualquier otro patrón, así se proporciona la flexibilidad para bloquear potencial contenido dañino. La lista de archivos patrón está pre configurada con una lista por defecto de archivos patrón:

- ✓ Archivos ejecutables (*.bat, *.com y *.exe).
- ✓ Archivos comprimidos (*.gz, *.rar y *.tar, *.tgz y *.zip).
- ✓ Librerías de enlace dinámico (*.dll).
- ✓ Aplicaciones html (*.hta).
- ✓ Archivos Microsoft Office (*.doc, *.ppt y *.xl?).
- ✓ Archivos Microsoft Works (*.wps).

- ✓ Archivos Visual Basic (*.vb?).
- ✓ Archivos screen saver (*.scr).
- ✓ Archivos de información de programa (*.wps).

XIII. Escáner de virus

Si el archivo ha pasado el módulo archivo patrón, entonces se le se aplica el scanner de virus; las definiciones de virus son almacenadas y actualizada periódicamente a través de FDN (Fundamentos de Cableado de Red). La unidad FortiGate usa las definiciones de virus para detectar y remover virus, gusanos, troyanos y otras amenazas de contenido.

La lista de virus muestra en orden alfabético las definiciones de virus FortiGuard actualizadas que se encuentran instaladas en la unidad FortiGate.

A) Heurístico: Finalmente, luego de haber pasado los tres módulos anteriores, el archivo entrante es sometido al módulo heurístico. El motor heurístico de la unidad FortiGate realiza pruebas en el archivo para detectar virus basándose en indicadores de comportamiento o en virus conocidos, es así que se puede detectar nuevos virus pero también se pueden producir resultados falsos positivos.

B) Cuarentena: La unidad FortiGate con disco duro puede poner en cuarentena a archivos bloqueados e infectados para ver el nombre y la información de estado de éstos; además pueden ser cargados automáticamente al análisis Fortinet. Para las unidades FortiGate que no

cuentan con disco duro, se puede configurar para que los archivos bloqueados e infectados sean enviados a la unidad FortiAnalyzer.

C) Protección Contra Intrusos: El sistema de prevención de intrusos (IPS) FortiGuard combina la detección de firmas y anomalías para descubrir y prevenir las intrusiones al sistema, con baja latencia y excelente confiabilidad. La unidad FortiGate puede grabar el tráfico sospechoso en logs (eventos), puede enviar alertas e-mail al sistema administrador y puede registrar, comunicar, soltar, restaurar y limpiar sesiones o paquetes sospechosos. También es posible habilitar o deshabilitar todas las firmas o anomalías en cada perfil de protección firewall.

D) Firmas: El IPS FortiGate compara el tráfico de red con los patrones contenidos en las firmas de ataques, las firmas de los ataques protegen la red de los ataques conocidos. La unidad FortiGate permite modelar nuevas firmas de acuerdo a las necesidades de la red además de las firmas predefinidas.

E) Decodificador de Protocolo: El IPS FortiGate usa la detección de anomalías para identificar el tráfico de red que intenta tomar ventaja de debilidades conocidas.

F) Anomalías: El IPS FortiGate usa la detección de anomalías para identificar el tráfico de red que no encaja en los patrones de tráfico predefinidos o conocidos; identifica cuatro tipos de anomalías estadísticas para los protocolos TCP (Protocolo de Control de Transmisión), UDP (Protocolo de Datagrama de Usuario) e ICMP (Protocolo de Mensajes de Control de Internet):

- Flooding

- Scan
- Source session limit
- Destination session limit

E) Filtro web

Los filtros web son aplicados en el siguiente orden:

1. URL de excepción.
2. URL bloqueada.
3. URL patrón bloqueada.
4. Categoría URL web bloqueada.
5. Contenido web bloqueado.
6. Filtro script.
7. Escaneo de virus.

F) Bloqueo de Contenido: Controla el contenido web al bloquear palabras o patrones específicos; si se habilita en el perfil de protección, la unidad FortiGate busca las palabras o patrones en las páginas web solicitadas, una coincidencia es encontrada cuando los valores asignados a las palabras son totales, si el valor de umbral definido de un usuario es excedido, la página web es bloqueada.

G) Filtro URL (Localizador Uniforme de Recursos): Permite o bloquea el acceso a URLs específicas, las cuales han sido añadidas a la lista de filtrado;

se añaden los patrones usando texto o expresiones regulares (caracteres wildcard).

La unidad FortiGate permite o bloquea páginas web comparándolas con las URLs o patrones especificados y despliega un mensaje de reemplazo a cambio indicando que la página no es accesible de acuerdo a las políticas de uso de Internet.

H) Filtro web FortiGuard: Es una solución de filtrado web administrada y provista por Fortinet que clasifica cientos de millones de páginas web dentro de un amplio rango de categorías que los usuarios pueden permitir, bloquear o monitorear.

La unidad FortiGate accede al punto de servicio FortiGuard - Web más cercano para determinar la categoría de una página solicitada, entonces continúa a la política firewall configurada por el usuario en la interfaz.

FortiGuard - Web abarca millones de valoraciones individuales de sitios web aplicándose a cientos de millones de páginas; las páginas son clasificadas y valoradas en 56 categorías que los usuarios pueden permitir, bloquear o monitorear; las categorías pueden ser añadidas o actualizadas según como el Internet evolucione.

La valoración de FortiGuard - Web es realizada mediante la combinación de métodos propietarios como análisis de texto, explotación de la estructura web y la intervención humana en la clasificación; los usuarios pueden notificar a los puntos de servicio FortiGuard - Web si piensan que una página no está categorizada correctamente además nuevos sitios son clasificados

rápidamente. Si se necesita acceder a un sitio web restringido se puede anular temporalmente la regla.

3. CAPÍTULO III: DESCRIPCIÓN DEL MODELO

3.1. ANÁLISIS DEL MODELO

3.1.1. Topología Inicial

En la Figura 12, muestra la topología inicial de la red interna de la Universidad Nacional de Trujillo, consta de un Switch Cisco Catalyst 2960 para la segmentación de las VLANs; también contiene un equipo Optimizador Exinda, para el control del ancho de banda; un equipo A10, que se encarga de proteger y balancear la carga hacia los servidores web; un equipo FortiGate 500 D, para la seguridad perimetral; un equipo Arbor, que se encarga de dropear o mitigar los ataque de denegación de servicio y un Router Juniper para la entrega del enlace de 200 Mbps. (Megabits por segundo).

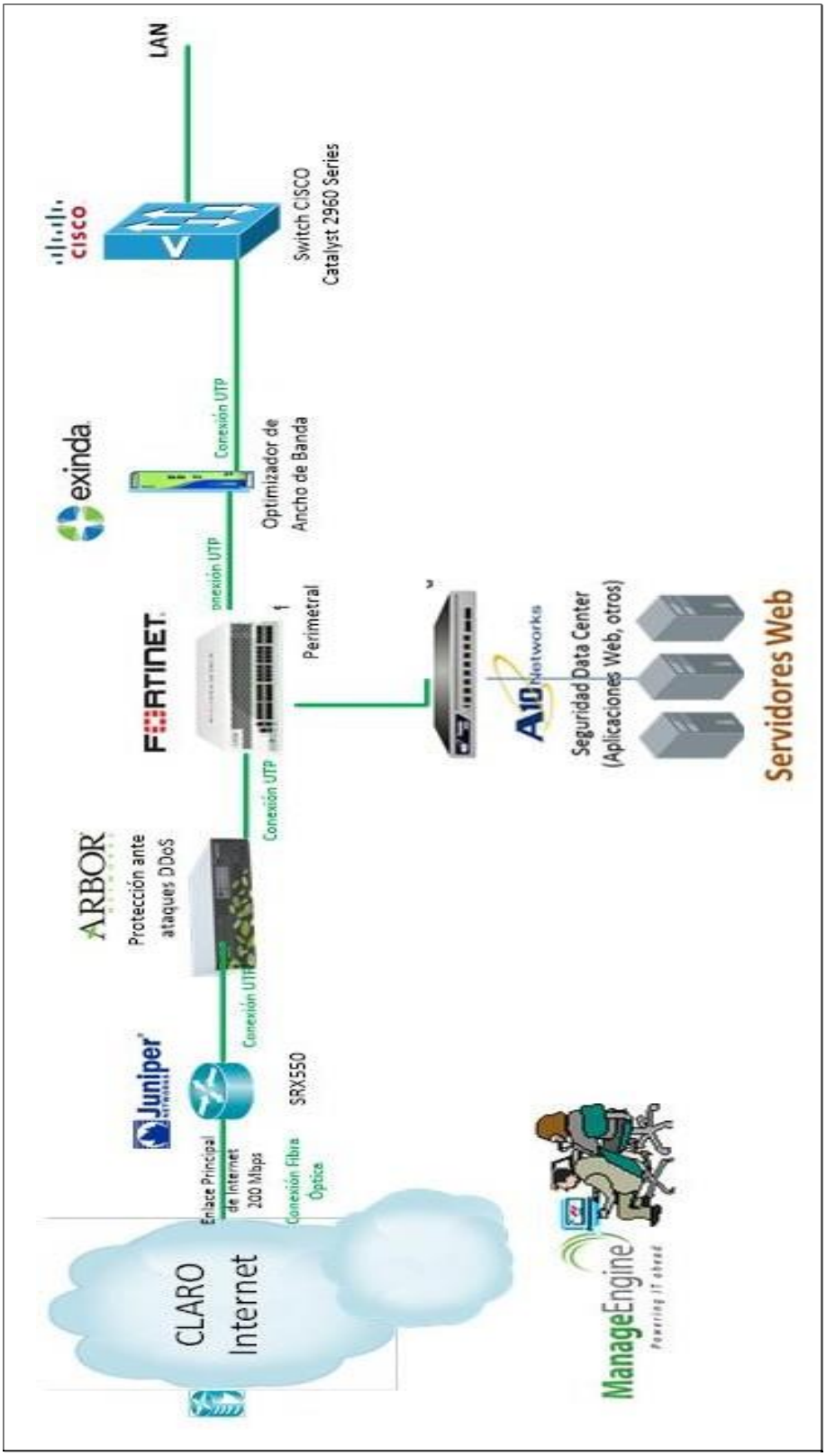


Figura 11: Topología Inicial de Red Interna de la Universidad Nacional de Trujillo

Fuente: Universidad Nacional de Trujillo

3.1.2 Requerimientos

Para la instalación del Firewall el cliente nos brindó la siguiente información:

Se debe brindar un Servicio de Seguridad Perimetral mediante la instalación de un equipo nuevo Firewall UTM. El equipo solicitado para la Universidad Nacional de Trujillo debe ser un equipo de seguridad en formato rack trabajando con las funciones de Firewall, Antivirus, AntiSpam, IPS-IDS, Filtro de Contenidos, Control de Aplicaciones, Proxy, Web Caching, y VPNs. A continuación se detallan las funcionalidades de la solución:

- Throughput (Resolución de problemas) de Firewall IPv4 (64 Bytes, UDP): 55 Gbps.
- Número Máximo de Sesiones Concurrentes (TCP): 12 Millones de sesiones.
- Nuevas sesiones por segundo (TCP): 300,000 conexiones.
- Throughput (Resolución de problemas) de IPS: 11 Gbps (Gigabits por segundo).
- Throughput (Resolución de problemas) de IPSec VPN (512 Bytes Packet): 50 Gbps.
- Throughput (Resolución de problemas) de Antivirus (Proxy): 4.3 Gbps (Gigabits por segundo).
- Interfaces: Mínimo de 16 interfaces 10/100/1000 RJ45 (Conexión LAN) y 2 interfaces 10/100/1000 RJ45 (Gestión).

- Capacidad de Almacenamiento: 240GB (GigBytes).
- Fuentes de Poder: AC o DC, redundantes hot-swap.
- Certificación: ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN.

En la Figura 12, muestra las rutas a configurar según la información brindad por el cliente.

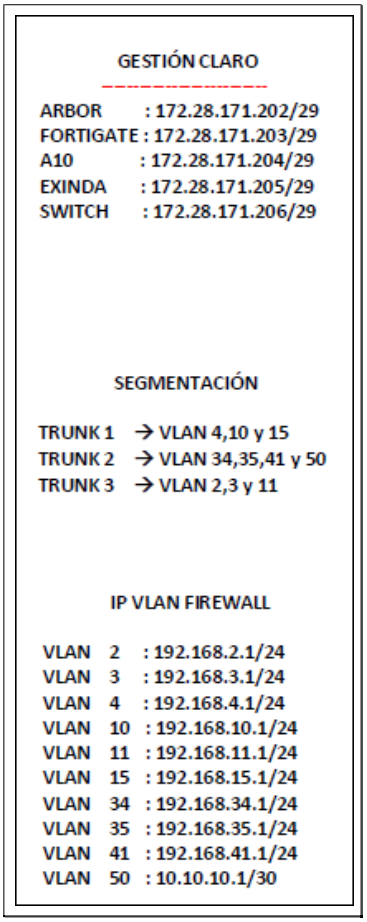


Figura 12: Configuración de VLANs de la Red Lan del Cliente.

Fuente: Universidad Nacional de Trujillo

3.1.3 Propuesta de solución Firewall

Según los requerimientos previos establecidos, se diseñó una solución de seguridad perimetral administrada, la cual se detalla a continuación:

3.1.3.1 Descripción técnica de equipos a instalar

- Basado en tecnología ASIC (Application-Specific Integrated Circuit) y que es capaz de brindar una solución de protección de contenido completo, es decir, cubre el análisis de contenido por categoría por web (contenido adulto, video/audio, redes sociales, etc).

- Capacidad de incrementar el rendimiento de VPN (Red Privada Virtual) a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).

- Capacidad de reensamblado de paquetes de datos en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).

- El equipo puede ser configurado en modo gateway (puerto de enlace) o en modo transparente en la red.

- En modo transparente, el equipo no requiere de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.

El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.

El equipo de seguridad debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento del mismo.

En La Figura 13. Se muestran las características técnicas de los equipos, los cuales se propusieron en relación a su capacidad de hardware.

	FG-1500D / 1500D-DC	FG-1500DT
Hardware Specifications		
Hardware Accelerated 10 GE SFP+ / GE SFP Slots	8	4
Hardware Accelerated GE SFP Slots	16	
Hardware Accelerated 10 GE RJ45 Ports	–	4
Hardware Accelerated GE RJ45 Ports	16	
GE RJ45 Management / HA Ports	2	
USB Ports (Client / Server)	1 / 1	
Console Port	1	
Onboard Storage	2x 240 GB	
Included Transceivers	2x SFP+ (SR 10GE)	
System Performance		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 55 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	80 / 80 / 55 Gbps	
Firewall Latency (64 byte, UDP)	3 µs	
Firewall Throughput (Packet per Second)	82.5 Mpps	
Concurrent Sessions (TCP)	12 Million	
New Sessions/Second (TCP)	300,000	
Firewall Policies	100,000	
IPsec VPN Throughput (512 byte)	50 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	20,000	
Client-to-Gateway IPsec VPN Tunnels	50,000	
SSL-VPN Throughput	4 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum)	10,000	
IPS Throughput (HTTP / Enterprise Mix) [1]	15 / 13 Gbps	
SSL Inspection Throughput [2]	10.5 Gbps	
Application Control Throughput [3]	12 Gbps	
NGFW Throughput [4]	7 Gbps	
Threat Protection Throughput [5]	5 Gbps	
CAPWAP Throughput [6]	20 Gbps	
Virtual Domains (Default / Maximum)	10 / 250	
Maximum Number of FortiAPs (Total / Tunnel)	4,096 / 1,024	
Maximum Number of FortiTokens	5,000	
Maximum Number of Registered Endpoints	8,000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

Figura 13: Datashep FortiGate 1500 D

Fuente: https://www.fortinet.com

3.1.3.2 Costos de la solución

En la Tabla 1, 2 y 3. Se detallan los costos del equipo FortiGate, para instalación y como respaldo (SPARE), también se muestran los costos de las licencias, el servicio de instalación, el servicio de capacitación y el soporte de 24x7 por 36 meses.

Tabla 1: Costos de los equipos FortiGate (Principal y Spare)

Equipo Fortinet FG - 1500 D				
Equipo de seguridad administrada - Costo de Venta		**Cantidad**	**Pago Único**	**Pago Total**
FG-1500D-BDL-950-12	Hardware (8 x 10GE SFP+ slots, 16 x GE SFP slots, 18 x GE RJ45 ports (including 16 x FortiASIC-acceleratedports, 2 x management/HA ports), FortiASIC NP6 and CP8 hardware accelerated, 240GB SSD onboardstorage) plus 1 year 24x7 Forticare and FortiGuard UTM Bundle	1	S/ 84,118.5	S/ 84,118.5
EQUIPO DE SEGURIDAD SPARE - COSTO DE VENTA				
FG-1500D-SPARE	FG-1500D Spare Soporte 8x5	1	S/ 50,981.4	S/ 50,981.4

Tabla 2: Costo de Instalación y configuración del equipo FortiGate

Servicio de Instalación y Configuración			
Equipo de seguridad administrada - Costo de Venta	**Cantidad**	**Pago Único**	**Pago Total**
Instalación y Configuración - Solución UTM	1	S/ 4,500.00	S/ 4,500.00

Tabla 3: Costo de Capacitación del equipo FortiGate

Servicio de Capacitación			
Equipo de seguridad administrada - Costo de Venta	**Cantidad**	**Pago Único**	**Pago Total**
Capacitación en la Solución de Seguridad Administrada FG-1500D - 4 horas para máx. 5 personas.	5	S/ 5,200.00	S/ 5,200.00

3.1.4 Diagrama de Actividades Secuenciales

Tabla 4: Diagrama de Actividades Secuenciales

FECHA	ACTIVIDAD	COMIENZO	FIN	TIEMPO ESTIMADO	DESCRIPCIÓN
Día 1	• Cableado y ordenamiento	15/08/2016; 7 am	15/08/2016; 10 pm	6 horas	Se va a realizar el cableado y ordenamiento de los equipos involucrados en el proyecto. El trabajo va a ser realizado en paralelo con el montaje y puesta en producción, para no afectar el servicio de manera prolongada se va a utilizar el cableado actual y al finalizar el día se realiza el cambio de cable.
	• Montaje y energización			3 horas	Se va a proceder con el montaje de los equipos y la energización.
	• Instalación Arbor			1 hora	Se va a proceder con la puesta en produccion del equipo perimetral Fortigate
	• Protocolo de pruebas del servicio			1 hora	Ejecución del protocolo de pruebas.
	• Capacitación Exinda			4 horas	Inducción a la herramienta de gestión de tráfico.
Día 2	• Instalación Fortinet	16/08/2016; 9 am	16/08/2016; 3:30 pm	1 hora	Se va a realizar la puesta en producción del equipo Arbor.
	• Protocolo de pruebas del servicio			1.5 horas	Ejecución del protocolo de pruebas.
	• Capacitación de A10			4 horas	Inducción a la protección de aplicaciiones Web.
Día 3	• Instalación A10	17/08/2016; 9 am	17/08/2016; 5 pm	1 hora	La afectación de servicio solo va a involucrar las páginas Web mas no la navegación hacia internet.
	• Protocolo de pruebas del servicio A10			1 hora	Ejecución del protocolo de pruebas.
	• Instalación Swicth Cisco 2960			1 hora	Instalación del Switch.
	• Protocolo de pruebas del servicio Switch			1 hora	Ejecución del protocolo de pruebas.
	• Capacitación Fortinet			4 horas	Inducción a la seguridad perimetral con Fortient
Día 4	• Instalación Exinda	18/08/2016; 9 am	18/08/2016; 3 pm	1 hora	Se va a realizar la puesta en producción del equipo Exinda.
	• Protocolo de pruebas del servicio			1 hora	Ejecución del protocolo de pruebas.
	• Capacitación de ARBOR			4 horas	Inducción de ataques de denegación de servicio y como el Arbor los mitiga.
Día 5	• Verificación del cableado de los equipos y ordenamiento.	19/08/2016; 9 am	19/08/2016; 4 pm	1 hora	Se va a verificar el cableado realizado con el ordenamiento (separadores y ordenadores en los rack para los equipos y cables. En el caso de la parte posterior la verificación del cableado entre Rack con tubo corrugado).
	• Checklist general de toda la solución			2 horas	Revisión del funcionamiento de la solución implementada.
	• Análisis y resolución de problemas			4 horas	La afectación de servicio es solamente si se presenta problemas con la solución que afecte la producción.

3.1.4.1 Requerimientos Físicos FORTINET:

Se realizó el siguiente despliegue para la instalación del FortiGate 1500 D:

- En las Figuras 14 y 15, se muestra el 2U rack mount en el gabinete que contiene un dimensionamiento (An x Al x Pr) de 438 x 89 x 554 mm y un peso de 14.7 kg.

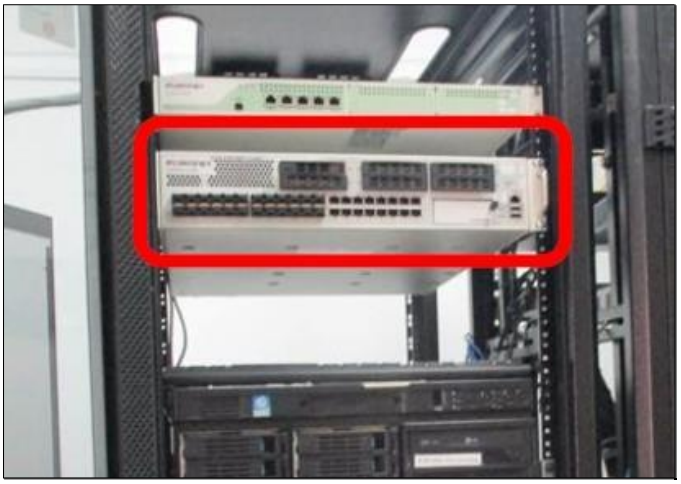


Figura 14: 2U Rack mount.

Fuente: Elaboración propia

Figura 15: FortiGate instalado en el gabinete

Fuente: Elaboración propia

Figura 16: Fuentes de alimentacion del equipo FortiGate

Fuente: Elaboración propia

3.1.4.2 Requerimientos para la configuración

Con respecto a la configuración del equipo, se requerirá proporcionar por parte de la Universidad Nacional de Trujillo la siguiente información:

- Subredes de cada facultad y administrativos y WLANs existentes.
- Subredes de la red de servidores, especificar IP (privada y pública) y la función de cada servidor.
- Especificar si se tiene un proxy y la ubicación del mismo en la topología.
- Rango de IPs públicas.
- Puertos que se requieren estén abiertos (permitidos).
- Políticas de restricción para IPs, protocolos y aplicaciones.

- Un punto de datos disponible para la gestión del equipo, a través de un puerto del Switch de su red interna.

3.1.4.3 Topología a Implementar

En la Figura 17, se muestra la topología propuesta para la solución el cual consta de un Switch Cisco Catalyst 2960 para la segmentación de las VLANs; también contiene un equipo Optimizador Exinda 4062, para el control del ancho de banda; un equipo A10, que se encarga de proteger y balancear la carga hacia los servidores web; un equipo FortiGate 1500 D, para la seguridad perimetral; un equipo Arbor 2002 APS, que se encarga de dropear o mitigar los ataque de denegación de servicio y un Router Juniper para la entrega del enlace de 320 Mbps. (Megabits por segundo).

La segmentación para la LAN (Red Área Local) se divide en las vlan 10, vlan 15, vlan 4, vlan 3, vlan 2, vlan 41y vlan 35, para un ordenamiento de redes a nivel interno; estos segmentos de VLANs están conectado al Switch Cisco Catalyst 2060. El equipo A10, se encuentra instalado para la protección del segmento de la VLAN de servidores. El dispositivo Arbor cubre la protección de ataques internos y externos, conectado entre el Router Juniper y el Firewall FortiGate. El equipo Exinda, se encuentra instalado entre el FortiGate y el Switch, para el control de optimización de ancho de banda para los segmentos de red y por último el equipo FortiGate, que se encarga de la protección perimetral de la red, con el control de servicios permitidos y el análisis de transmisión de datos a nivel interno y externo.

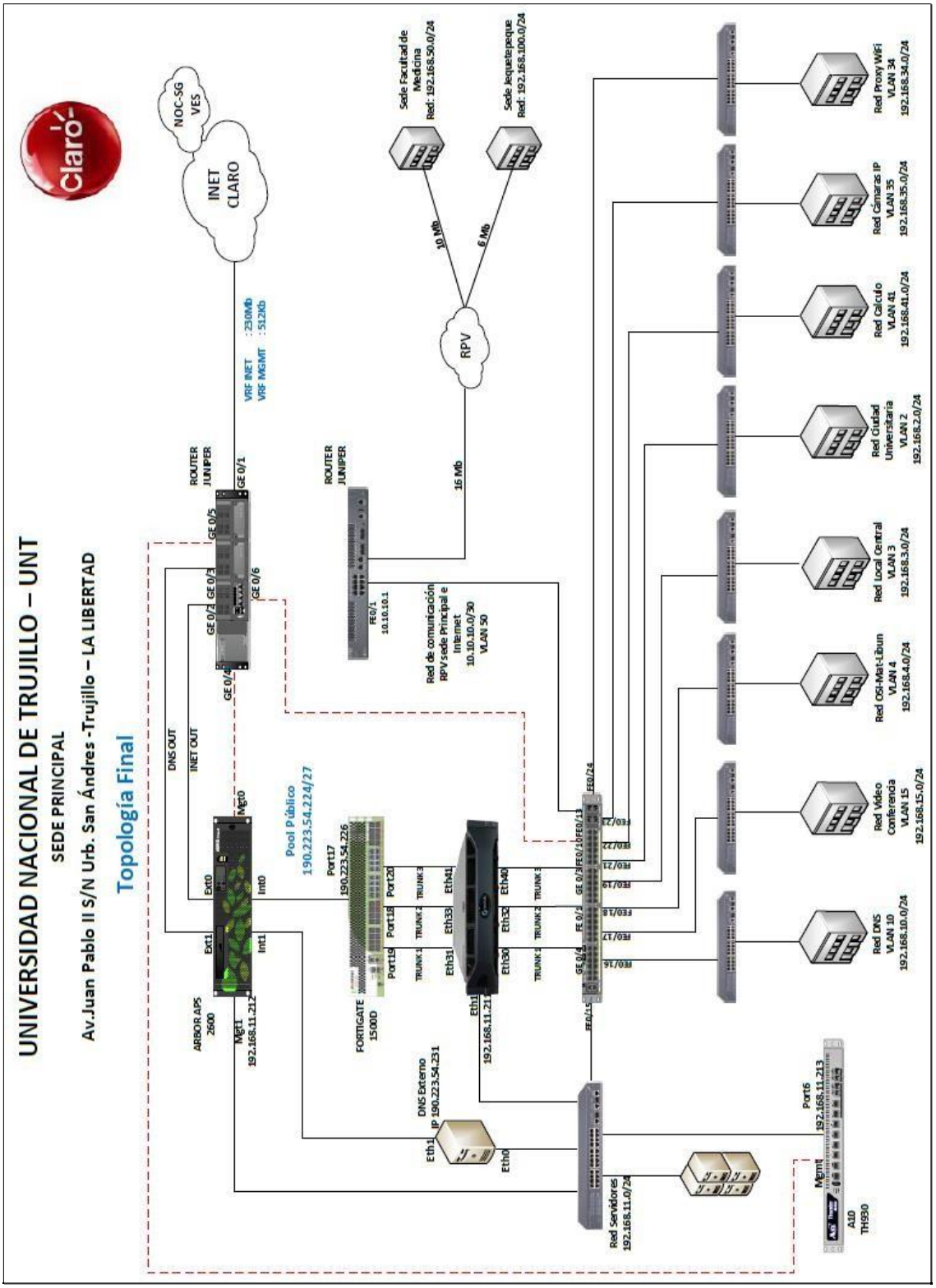


Figura 17: Topología Final de la red LAN de la Universidad Nacional de Trujillo

Fuente: Elaboración propia

3.1.4.4 Cronograma

A continuación se detalla el cronograma con las fechas de instalación, configuración y realización del protocolo de pruebas de cada solución involucrada:

Tabla 5: Cronograma de actividades

FECHA	ACTIVIDAD	OBSERVACION
Día 1	• Definición de la topología final • Instalación del equipamiento • Firma de acta de instalación • Capacitación FORTINET	Se validará el espaciamiento final y cableado a realizar, se procederá a instalar físicamente los equipos.
Día 2	• Configuración del FortiGate	Se procederá a configurar el equipo FortiGate previo a la migración.
Día 3	• Migración del servicio • Ordenamiento del cableado • Protocolo de pruebas del servicio • Firma de acta del servicio	Según coordinaciones con el cliente se realizará la migración, pruebas del servicio en general.
Día 4	• Verificaciones finales	Luego de la migración se probara el buen funcionamiento de los equipos y el servicio.
Día 5	• Verificaciones finales	Día adicional para verificar el buen funcionamiento del servicio.

3.1.4.5 Plan de Implementación

Esta etapa se centra en el plan de trabajo respecto a la instalación y configuración de la solución a trabajar, se detallará las implicancias de la solución desde la instalación física, conectividad, configuración, el protocolo de pruebas y puesta en marcha de los servicios.

Instalación – Configuración – Protocolo de Pruebas

FORTIGATE

A continuación se detallara el proceso de instalación, configuración y la validación con un protocolo de pruebas del equipo FortiGate:

A) INSTALACIÓN

El proceso de instalación implica la colocación del equipo en el gabinete y lugar establecido, a este equipo se le colocará un rotulo (sticker) en el cual aparecerá un número gratuito para realizar configuración, consultas o algún inconvenientes con el servicio que implica el equipo.

También se le colocará rótulos en las interfaces del equipo para poder distinguir las conexiones de manera rápida y esto ayudar en alguna avería física.

Se tomaran dos fotos de frente y dos en la parte posterior del equipo para fines de realizar un informe.

B) CONFIGURACIÓN

Se realizará la configuración de acuerdo a las bases establecidas y de acuerdo a los requerimientos del cliente, a continuación se detallará los pasos de la configuración (según los requerimientos del cliente estos pasos pueden cambiar):

- ✓ Revisión status del equipo: firmware, licencias.
- ✓ Configuración de direccionamiento IP, interfaces y enrutamiento.
- ✓ Configuración de servicios de red (DNS, DHCP, SNMP, NTP).
- ✓ Configuración de la protección de la red (NAT, IPS, Firewall).
- ✓ Configuración de la protección de WEB (Web filtering).
- ✓ Configuración de VPNs.
- ✓ Configuración de la gestión remota de CLARO.
- ✓ Configuración de la gestión del cliente.
- ✓ Creación de usuarios para el cliente.

C) PROTOCOLO DE PRUEBAS

Se realizará un protocolo de pruebas con la finalidad de validar el buen funcionamiento del equipo, este protocolo de pruebas se realizará conjuntamente con el cliente el cual firmara el documento validando los resultados obtenidos, dicho protocolo de pruebas tendrá por objetivo probar la correcta configuración y el buen funcionamiento del equipo FORTIGATE; en lo que respecta a configuraciones se probará:

- ✓ Probar la redundancia de las fuentes
- ✓ Probar las reglas del Firewall, NAT, WebFiltering y VPN.
- ✓ Probar la funcionalidad de los servicios críticos.

3.1.4.6 Plan de Migración

Las siguientes acciones describen las actividades a realizar para la migración:

Tabla 6: Plan de Migración

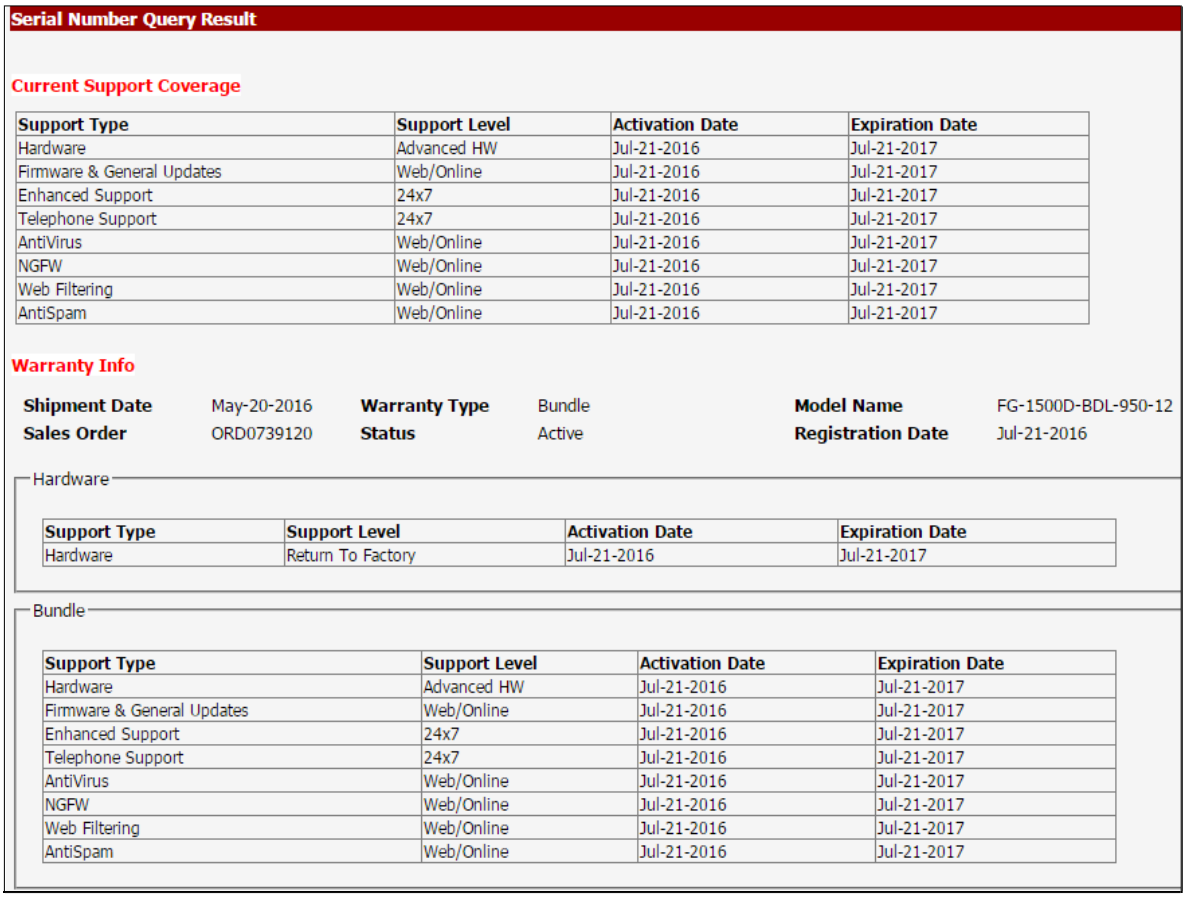
Tarea	Descripción	Tiempo Estimado
PRIMERA FASE – Puesta en Operación de los equipos Fortinet		
1	Realizar las conexiones de los cableados desde el switch Core hacia el equipo Optimizador Exinda	15 min
2	Revisar estatus de las interfaces del Optimizador para confirmar operatividad sin errores.	10 min
3	Pruebas de Conectividad hacia Internet	15 min
4	Pruebas de Servicios del Cliente	30 min
5	Revisión de estatus de equipo Fortinet: CPU, memoria, interfaces y políticas.	10 min
6	Revisión de estatus de equipo Exinda: CPU, memoria, interfaces y políticas.	10 min
7	Revisión de estatus de equipo Arbor Networks: CPU, memoria, interfaces y políticas.	10 min
SEGUNDA FASE - Puesta en operación del equipo A10 Networks		
8	Habilitar las políticas en el Fortinet para apuntar al WAF de A10 Networks (según la topología a definir con el cliente)	15 min
9	Pruebas de conectividad a servidores	10 min
10	Prueba de acceso a servicios de servidores	10 min
11	Prueba de servicios de servidores desde Internet	30 min
12	Revisión de estatus de equipo Exinda: CPU, memoria, interfaces y políticas.	10 min
13	Protocolo de Pruebas del equipo A10 networks	30 min
14	Pruebas finales de servicios	15 min

3.2 CONSTRUCCIÓN DEL MODELO

3.2.1 FortiGate 1500D

3.2.1.2 Licenciamiento

El tipo de licencia es Bundle, es decir, la licencia adquiere una licencia temporal (1 mes) cuando se culmine el contrato hasta que se tenga un acuerdo de renovación de servicios por parte del cliente y el proveedor; en la Figura 18, muestra las características que incluye esta licencia adquirida por la universidad.



Serial Number Query Result

Current Support Coverage

Support Type	Support Level	Activation Date	Expiration Date
Hardware	Advanced HW	Jul-21-2016	Jul-21-2017
Firmware & General Updates	Web/Online	Jul-21-2016	Jul-21-2017
Enhanced Support	24x7	Jul-21-2016	Jul-21-2017
Telephone Support	24x7	Jul-21-2016	Jul-21-2017
AntiVirus	Web/Online	Jul-21-2016	Jul-21-2017
NGFW	Web/Online	Jul-21-2016	Jul-21-2017
Web Filtering	Web/Online	Jul-21-2016	Jul-21-2017
AntiSpam	Web/Online	Jul-21-2016	Jul-21-2017

Warranty Info

Shipment Date	May-20-2016	**Warranty Type**	Bundle	**Model Name**	FG-1500D-BDL-950-12
Sales Order	ORD0739120	**Status**	Active	**Registration Date**	Jul-21-2016

Hardware

Support Type	Support Level	Activation Date	Expiration Date
Hardware	Return To Factory	Jul-21-2016	Jul-21-2017

Bundle

Support Type	Support Level	Activation Date	Expiration Date
Hardware	Advanced HW	Jul-21-2016	Jul-21-2017
Firmware & General Updates	Web/Online	Jul-21-2016	Jul-21-2017
Enhanced Support	24x7	Jul-21-2016	Jul-21-2017
Telephone Support	24x7	Jul-21-2016	Jul-21-2017
AntiVirus	Web/Online	Jul-21-2016	Jul-21-2017
NGFW	Web/Online	Jul-21-2016	Jul-21-2017
Web Filtering	Web/Online	Jul-21-2016	Jul-21-2017
AntiSpam	Web/Online	Jul-21-2016	Jul-21-2017

Figura 18: Caracteristicas de Licencia

Fuente: https://www.fortinet.com

Luego de realizar la compra se procedio a realizar el registro correspondiente y la descripcion que se le otorga a la licencia a nombre de la Universidad Nacional de Trujillo, asi como se describe en la Figura 19.

Figura 19: Descripción y Registro de Licenciamiento

Fuente: Elaboracion Propia

3.2.1.3 Información del Sistema

En la Figura 20, se muestra la descripción del equipo (FGT-UNT), el número de serial (SN: FG1K5D3I16800082) y la versión de firmware (5.2.7).

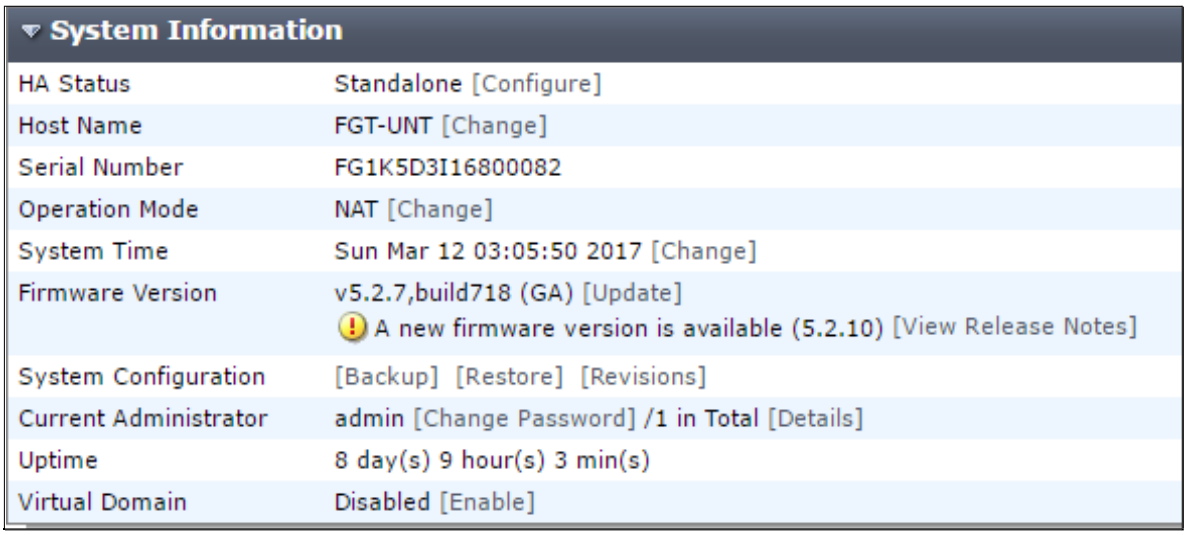


Figura 20: Información del Sistema

Fuente: Elaboración propia

3.2.1.4 Interfaces Configuradas

En la Figura 21 y 22. Se muestra el direccionamiento IP asignado a cada interface en el FortiGate.

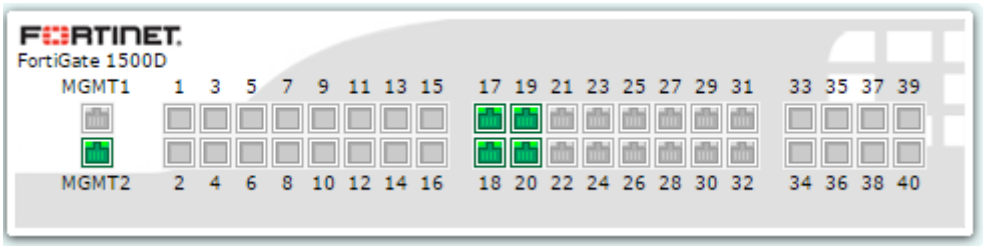


Figura 21: Puertos Conectados del FortiGate

Fuente: Elaboración propia

port17 (INET-CLARO)	190.223.54.226 255.255.255.224	Physical	PING HTTPS SSH SNMP
port18	0.0.0.0 0.0.0.0	Physical	PING HTTPS SSH SNMP
CamarasIP	192.168.35.1 255.255.255.0	VLAN	
ProxyWifi	192.168.34.1 255.255.255.0	VLAN	
RPV_VALLE_MED	10.10.10.1 255.255.255.252	VLAN	PING
RedCalculo	192.168.41.1 255.255.255.0	VLAN	
port19	0.0.0.0 0.0.0.0	Physical	
DNS	192.168.10.2 255.255.255.0	VLAN	
Osi-Mat-Libun	192.168.4.1 255.255.255.0	VLAN	
VideoConf	192.168.15.1 255.255.255.0	VLAN	
port20	0.0.0.0 0.0.0.0	Physical	
CiudadUniv	192.168.2.1 255.255.255.0	VLAN	
LocalCentral	192.168.3.1 255.255.255.0	VLAN	
Servidores	192.168.11.1 255.255.255.0	VLAN	PING HTTPS SSH SNMP

Figura 22: Direccionamiento IP

Fuente: Elaboración propia

- ✓ Interfaz MGMT2: Para la administración del equipo de forma remota se configuró en el firewall FortiGate la IP 172.28.171.203/28, con los protocolos de servicios activados para la gestión (PING, HTTPS, SSH y SNMP).

- ✓ Puerto 17: Dicha interfaz está conectada al enlace WAN (Red de Área Amplia) del Router, para el acceso hacia la salida del Internet. Se configuró la IP 190.223.54.226/28 para la interfaz y la gestión por los protocolos de servicio (PING, HTTPS, SSH y SNMP).

- ✓ Puerto 18: Se configuró los segmentos 192.168.35.1/24, 192.168.34.1/24,10.10.10.1/30 y 192.168.41.1/24; ya que cada segmento descrito cuenta con su descripción de VLAN: CamarasIP, ProxyWifi, RPV_VALLE_MED y RedCalculo respectivamente.

- ✓ Puerto 19: Se configuró los segmentos 192.168.10.2/24, 192.168.4.1/24, y 192.168.15.1/24; ya que cada segmento descrito cuenta con su descripción de VLAN: DNS, Osi_Mat_Libun y VideoConf respectivamente.

- ✓ Puerto 20: Se configuró los segmentos 192.168.2.1/24, 192.168.3.1/24, y 192.168.11.1/24; ya que cada segmento descrito cuenta con su descripción de VLAN: CiudadUniv, LocalCentral, y Servidores respectivamente.

Nota: Las interfaces que no se utilizan se han deshabilitado administrativamente.

3.2.1.5. Configuración de Administración

En la Figura 23. Se muestran los puertos lógicos que utiliza el firewall para la gestión.

Cabe aclarar que se modificó los puertos utilizados para la conexión al equipo siendo los siguientes:

- Acceso web vía (https) puerto 10443.
- Acceso vía (ssh) puerto 2222.

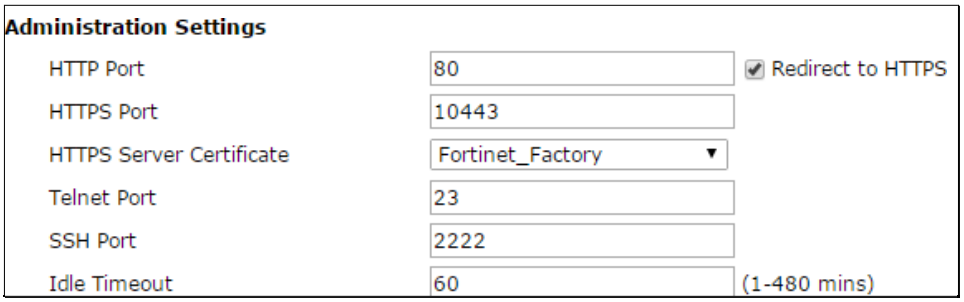


Figura 23: Acceso para la Gestión del FortiGate

Fuente: Elaboración propia

A) Tabla de Enrutamiento

En el FortiGate se ha creado para la navegación hacia internet una ruta estática que se conoce como default route, se ha creado una tabla de ruteo en base a las necesidades de la red del cliente, como se muestra en la Figura 24, los puertos de enlaces configurados para la salida de Internet con cada VLAN segmentada.

El FortiGate selecciona la mejor ruta para un paquete evaluando la información en la tabla de ruteo. Generalmente esto es, la ruta con menor distancia. Una vez evaluada las tablas de ruteo, el FortiGate crea una sub-tabla dentro de la tabla general llamada "**Forwarding Table**" la cual es utilizada para enviar los paquetes según la información de esta tabla de forwarding.

IP/Netmask	Gateway	Device	Comment
0.0.0.0 0.0.0.0	190.223.54.225	port17	
192.168.16.0 255.255.255.0	192.168.3.8	LocalCentral	
172.28.129.32 255.255.255.224	172.28.171.201	mgmt2	
192.168.100.0 255.255.255.0	10.10.10.2	RPV_VALLE_MED	Sede Valle
192.168.50.0 255.255.255.0	10.10.10.2	RPV_VALLE_MED	Sede Medicina

Figura 24: Puertos de Enlaces (Default Route)

Fuente: Elaboración propia

B) Configuración SNMP (Protocolo Simple de Administración de Red)

Se tiene un equipo OpManager, en el área del centro de operaciones de seguridad de red (NSOC), este servidor está dedicado para la recepción de traps SNMP, y recopilar la información de los recursos del equipo FortiGate. Como bien muestra la Figura 25, se tiene la dirección IP del servidor configurado en el firewall para brindar la información y registrar los traps que se envían al servidor de monitoreo.

Figura 25: Configuracion SNMP (Protocolo Simple de Administración de Red)

Fuente: Elaboración propia

C) Configuración de usuarios de Administración

En la Figura 26 y 27. Se muestra las cuentas de administración de los usuarios internos para la administración del equipo FortiGate, de acuerdo a los perfiles indicados por el cliente (Administrador y monitor).

Name	Trusted Hosts	Profile	Type
admin	0.0.0.0/0	super_admin	Local
dsicunt	0.0.0.0/0	monitor	Local
wlopez	0.0.0.0/0	super_admin	Local

Figura 26: Cuentas de Administración

Fuente: Elaboración propia

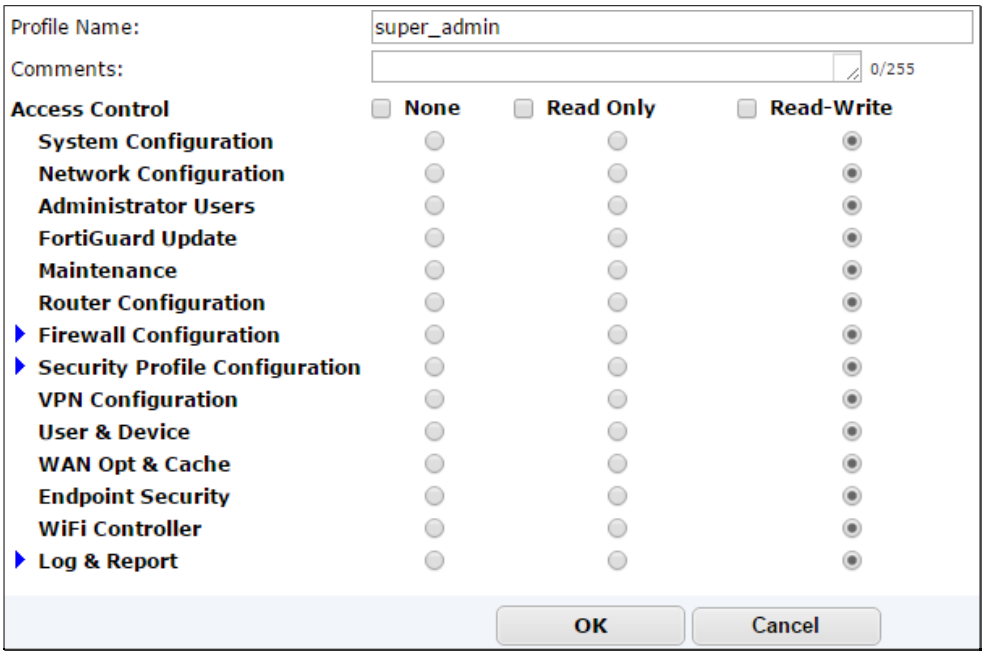


Figura 27: Perfiles de Admistración

Fuente: Elaboración propia

D) Políticas de Firewall

Se crearon las políticas de firewall requeridas de acuerdo al esquema que se planteó en la implementación, como se muestran en las Figuras 28 y 29.

10	port17 (INET-CLARO)	Servidores	all	Grp_Picfedu-DSpace	always	HTTPS HTTP TCP/8080
11	port17 (INET-CLARO)	Servidores	all	Grp_VIP_Web2	always	SG_Web2
12	port17 (INET-CLARO)	Servidores	all	Grp_VIP_OpenfireRadius	always	SG_Openfire
13	port17 (INET-CLARO)	Osi-Mat-Libun	Grp_IPBlock	all	always	ALL
14	port17 (INET-CLARO)	Osi-Mat-Libun	all	Grp_VIP_SrvDesarrollo	always	HTTPS TCP/5432 TCP/8080
15	port17 (INET-CLARO)	Osi-Mat-Libun	all	VIP_Srv_Alumnos_50123 VIP_Srv_Alumnos_5901	always	TCP/50123 TCP/5901
16	port17 (INET-CLARO)	CiudadUniv	Grp_IPBlock	all	always	ALL
17	port17 (INET-CLARO)	CiudadUniv	all	VIP_Postgrado_80 VIP_AdminisionApp_80	always	HTTP
18	port17 (INET-CLARO)	LocalCentral	Grp_IPBlock	all	always	ALL
19	port17 (INET-CLARO)	LocalCentral	all	VIP_Svr-Siaf_3306	always	MYSQL
20	port17 (INET-CLARO)	VideoConf	Grp_IPBlock	all	always	ALL
21	port17 (INET-CLARO)	VideoConf	all	VIP_VideoConf_80	always	HTTP
22	port17 (INET-CLARO)	CamarasIP	Grp_IPBlock	all	always	ALL
23	port17 (INET-CLARO)	CamarasIP	all	VIP_CamaraWeb_80	always	HTTP
24	port17 (INET-CLARO)	RedCalculo	Grp_IPBlock	all	always	ALL

Figura 28: Politica de Navegacion – NAT

Fuente: Elaboracion propia

Seq.#	From	To	Source	Destination	Schedule	Service
75	CiudadUniv	LocalCentral	Red_2	Red_3	always	ALL
76	LocalCentral	CamarasIP	Red_3	Red_35	always	ALL
77	LocalCentral	ProxyWifi	Red_3	Red_34	always	ALL
78	LocalCentral	Osi-Mat-Libun	Red_3	Red_4	always	ALL
79	LocalCentral	RedCalculo	Red_3	Red_41	always	ALL
80	LocalCentral	VideoConf	Red_3	Red_15	always	ALL
81	LocalCentral	CiudadUniv	Red_3	Red_2	always	ALL
82	CamarasIP	port17 (INET-CLARO)	Red_35	all	always	ALL
83	ProxyWifi	port17 (INET-CLARO)	Red_34	all	always	ALL
84	RedCalculo	port17 (INET-CLARO)	Red_41	all	always	ALL
85	VideoConf	port17 (INET-CLARO)	Red_15	all	always	ALL
86	CiudadUniv	port17 (INET-CLARO)	Red_2	all	always	ALL
87	LocalCentral	port17 (INET-CLARO)	Red_LocalCentral-Cestunt	all	always	ALL
88	LocalCentral	port17 (INET-CLARO)	Red_3	all	always	ALL
89	Osi-Mat-Libun	port17 (INET-CLARO)	Red_4	all	always	ALL
90	DNS	port17 (INET-CLARO)	Red_DNS	all	always	ALL
91	Servidores	port17 (INET-CLARO)	Red_Servidores	all	always	ALL
92	Servidores	CamarasIP	Red_Servidores	Red_35	always	ALL
93	Servidores	ProxyWifi	Red_Servidores	Red_34	always	ALL
94	Servidores	RedCalculo	Red_Servidores	Red_41	always	ALL

Figura 29: Politicas de Navegacion hacia Internet

Fuente: Elaboración propia

E) Filtrado Web

Como se muestra en la Figura 30. A solicitud de la Universidad solo se ha procedido con el bloqueo del acceso a internet de las siguientes categorias:

- ✓ Pornografía
- ✓ Páginas proxy
- ✓ Sitios maliciosos

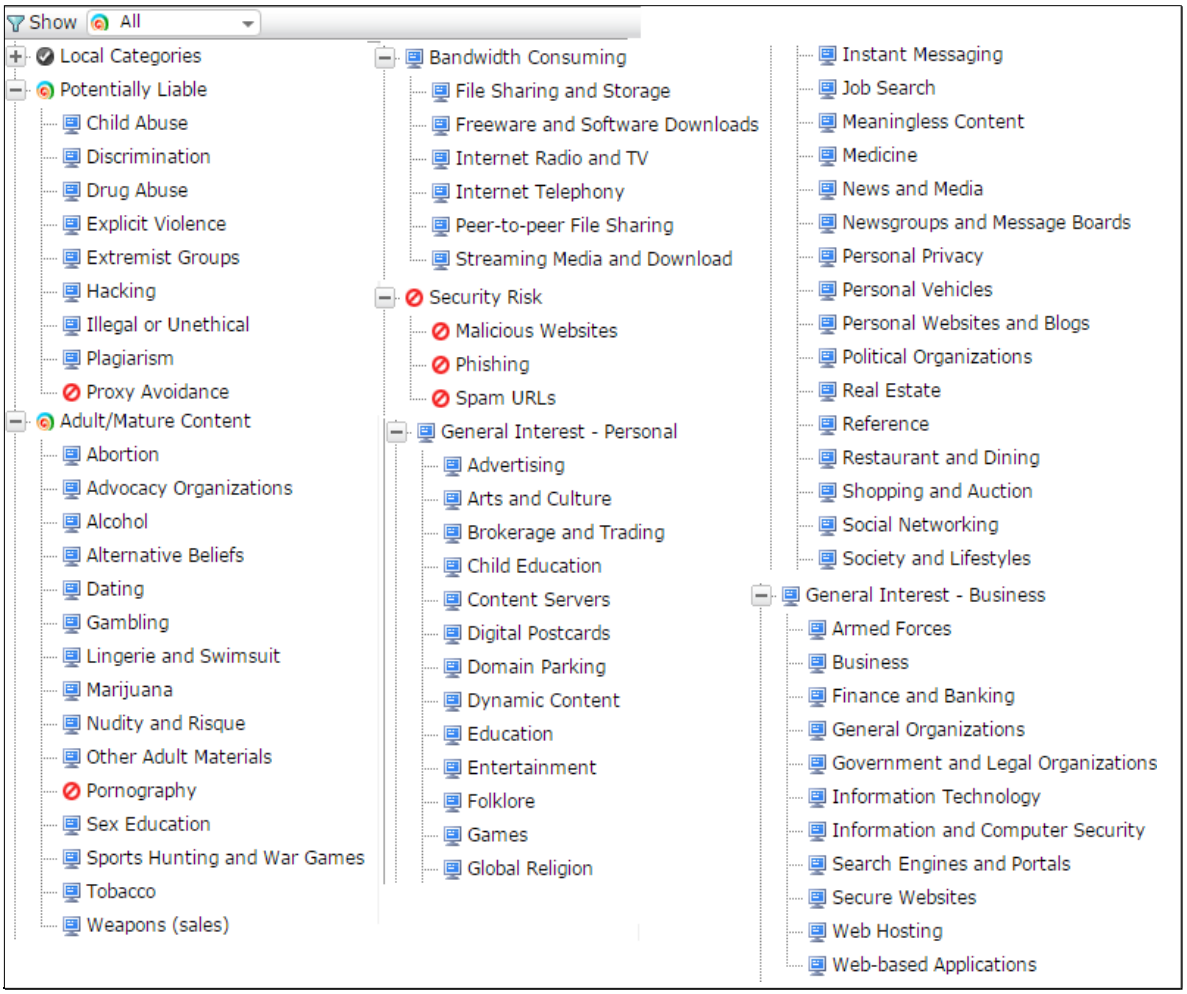


Figura 30: Bloqueo de Categorías

Fuente: Elaboración propia

F) Antivirus Perimetral

Se ha creado un perfil general de Antivirus el cual va a analizar por firmas la presencia de virus, como se muestra en la Figura 30, esta configuración realizada permitirá bloquear las conexiones Botnet y C&C Server.

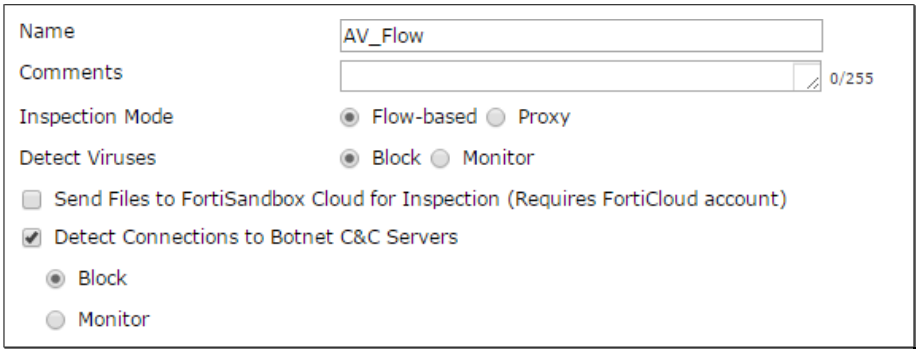


Figura 31: Configuración Antivirus

Fuente: Elaboración propia

G) Control de Aplicaciones

El control de tráfico de origen o destino se puede realizar mediante perfiles de control de aplicaciones, según lo impuesto por el cliente solo se bloqueó las categorías botnet, p2p y proxy, estos tipos de categorías solo bloquearan contenido malicioso que pueda alterar la red del cliente, como se muestra en la Figura 32.

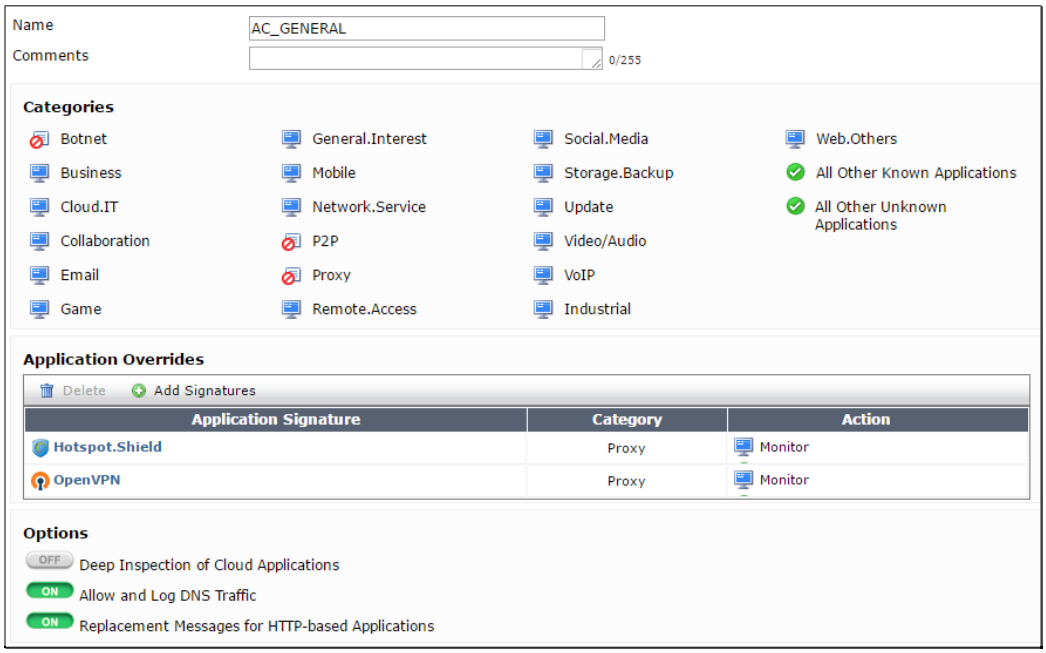


Figura 32: Control de Aplicaciones

Fuente: Elaboración propia

H) Protección de Intrusos

Se ha configurado el perfil de protección contra intrusos el cual ha sido asignado a la publicación de los servicios del cliente, en la Figura 33 se observa que en la configuración requerida para el cliente se impuso más de 1143 firmas para el análisis de ataques. Cuando el análisis de paquetes de datos coincida con una de las firmas automáticamente se bloqueara.

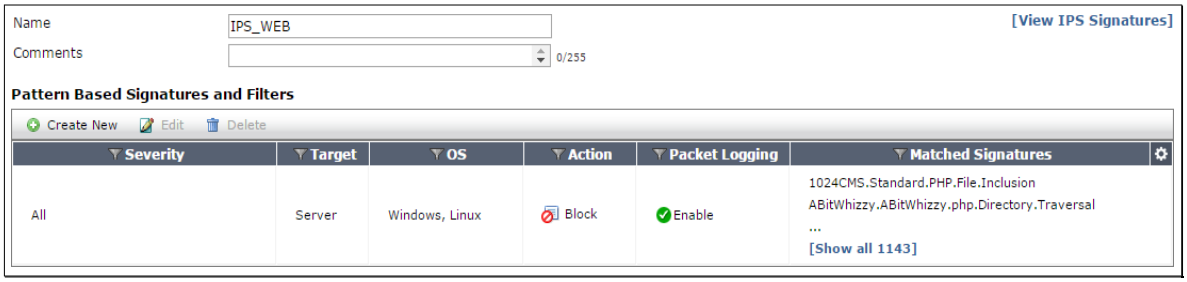


Figura 33: Configuración IPS

Fuente: Elaboración propia

3.3 REVISIÓN Y CONSOLIDACIÓN DE RESULTADOS

3.3.1. CPU y Memoria

El parámetro acorde para un rendimiento óptimo del equipo debe cubrir un promedio de consumo de CPU de 70 % y de memoria un 80%. Como se muestra en la Figura 34, los resultados se encuentran dentro de los parámetros establecidos.

Figura 34: Consumo de CPU y Memoria

Fuente: Elaboración propia

3.3.2 Verificación del estado de las interfaces

Se muestra el modo de negociación de las interfaces del FortiGate, así como la verificación de errores y posibles colisiones de tramas.

Para la cual se muestra la información de las interfaces del FortiGate a un nivel más detallado.

Como se muestra en la Figura 35, no se verificó errores ni colisiones en la interfaz, la velocidad de navegacion esta en 1000 Full Duplex, configurada para la salida hacia Internet evidenciando la navegacion sin latencia.

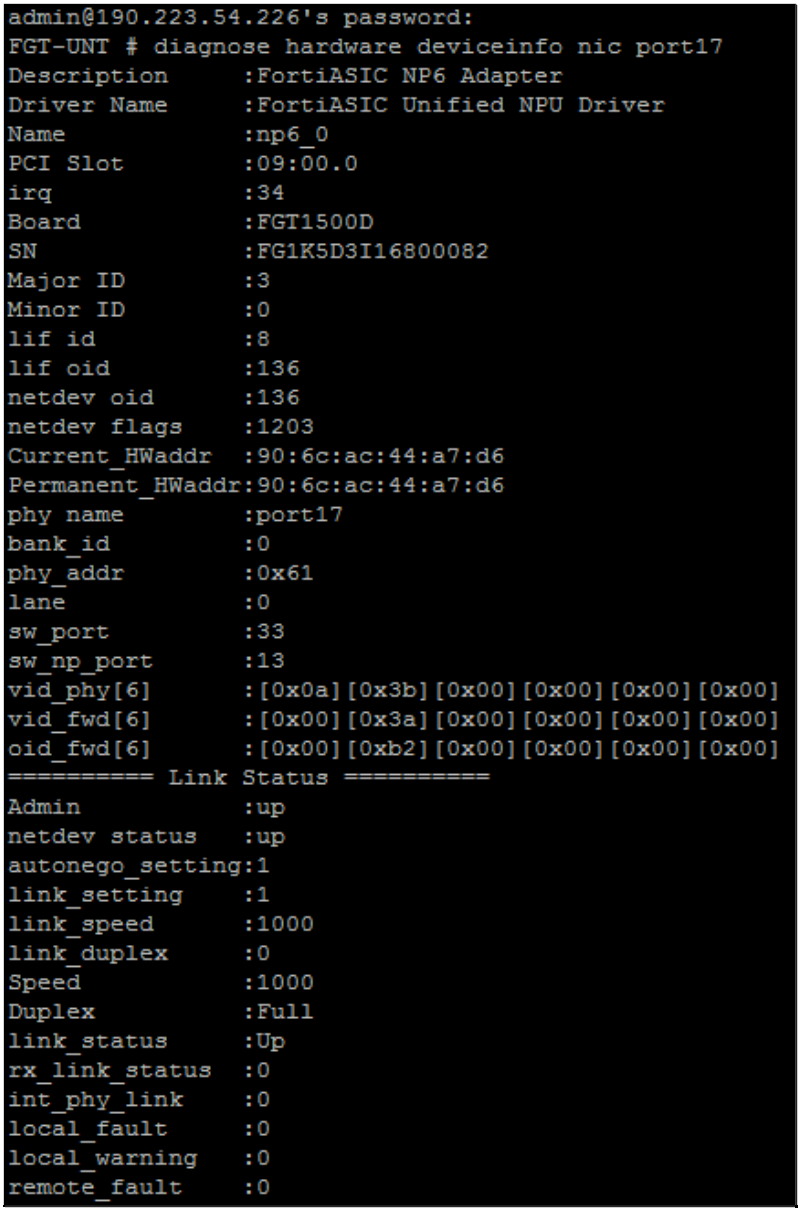
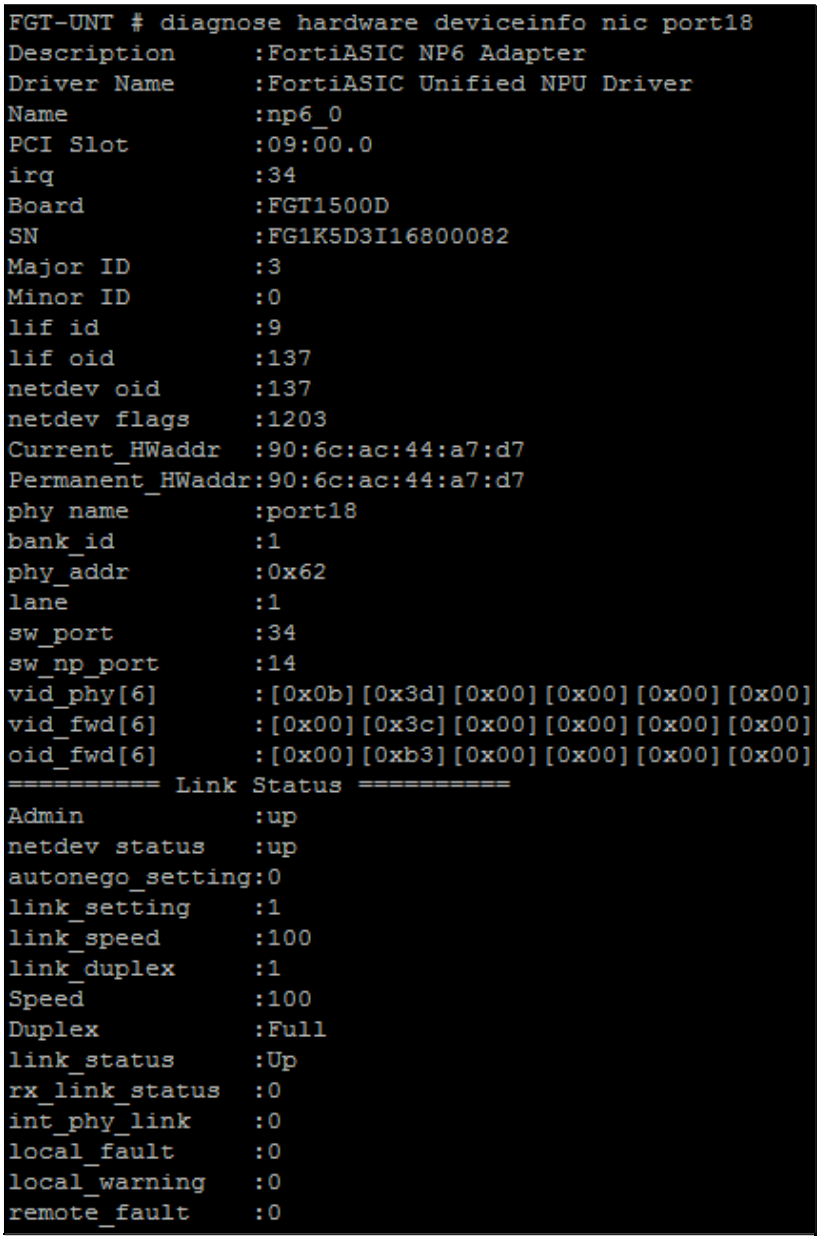


Figura 35: Puerto 17 – Diagnostico

Fuente: Elaboración propia

Como se muestra en la Figura 36, no se verificó errores ni colisiones en la interfaz, la velocidad de navegacion esta en 1000 Full Duplex, configurada para la conectividad de las segmentacion de VLANs: CamarasIP, ProxyWifi, Rpv_Valle_MED y RedCalculo.



```
FGT-UNT # diagnose hardware deviceinfo nic port18
Description     :FortiASIC NP6 Adapter
Driver Name     :FortiASIC Unified NPU Driver
Name            :np6_0
PCI Slot        :09:00.0
irq             :34
Board           :FGT1500D
SN              :FG1K5D3I16800082
Major ID        :3
Minor ID        :0
lif id          :9
lif oid         :137
netdev oid      :137
netdev flags    :1203
Current_HWaddr  :90:6c:ac:44:a7:d7
Permanent_HWaddr:90:6c:ac:44:a7:d7
phy name        :port18
bank_id         :1
phy_addr        :0x62
lane            :1
sw_port         :34
sw_np_port      :14
vid_phy[6]      :[0x0b][0x3d][0x00][0x00][0x00][0x00]
vid_fwd[6]      :[0x00][0x3c][0x00][0x00][0x00][0x00]
oid_fwd[6]      :[0x00][0xb3][0x00][0x00][0x00][0x00]
========== Link Status ==========
Admin           :up
netdev status   :up
autonego_setting:0
link_setting    :1
link_speed      :100
link_duplex     :1
Speed           :100
Duplex          :Full
link_status     :Up
rx_link_status  :0
int_phy_link    :0
local_fault     :0
local_warning   :0
remote_fault    :0
```

Figura 36: Puerto 18 – Diagnostico

Fuente: Elaboración propia

Como se muestra en la Figura 37, no se verificó errores ni colisiones en la interfaz, la velocidad de navegacion esta en 1000 Full Duplex, configurada para la conectividad de las segmentacion de VLANs: DNS, Osi-Mat-Libun y VideoConf.

```
FGT-UNT # diagnose hardware deviceinfo nic port19
Description     :FortiASIC NP6 Adapter
Driver Name     :FortiASIC Unified NPU Driver
Name            :np6_0
PCI Slot        :09:00.0
irq             :34
Board           :FGT1500D
SN              :FG1K5D3I16800082
Major ID        :3
Minor ID        :0
lif id          :10
lif oid         :138
netdev oid      :138
netdev flags    :1203
Current_HWaddr  :90:6c:ac:44:a7:d8
Permanent_HWaddr:90:6c:ac:44:a7:d8
phy name        :port19
bank_id         :2
phy_addr        :0x63
lane            :2
sw_port         :35
sw_np_port      :15
vid_phy[6]      :[0x0c][0x3f][0x00][0x00][0x00][0x00]
vid_fwd[6]      :[0x00][0x3e][0x00][0x00][0x00][0x00]
oid_fwd[6]      :[0x00][0xb4][0x00][0x00][0x00][0x00]
========== Link Status ==========
Admin           :up
netdev status   :up
autonego_setting:1
link_setting    :1
link_speed      :1000
link_duplex     :0
Speed           :1000
Duplex          :Full
link_status     :Up
rx_link_status  :0
int_phy_link    :0
local_fault     :0
local_warning   :0
remote_fault    :0
```

Figura 37: Puerto 19 – Diagnostico

Fuente: Elaboración propia

Como se muestra en la Figura 38, no se verificó errores ni colisiones en la interfaz, la velocidad de navegacion esta en 1000 Full Duplex, configurada para la conectividad de las segmentacion de VLANs: CiudadUniv, LocalCentral y Servidores.

```
FGT-UNT # diagnose hardware deviceinfo nic port20
Description     :FortiASIC NP6 Adapter
Driver Name     :FortiASIC Unified NPU Driver
Name            :np6_0
PCI Slot        :09:00.0
irq             :34
Board           :FGT1500D
SN              :FG1K5D3I16800082
Major ID        :3
Minor ID        :0
lif id          :11
lif oid         :139
netdev oid      :139
netdev flags    :1203
Current_HWaddr  :90:6c:ac:44:a7:d9
Permanent_HWaddr:90:6c:ac:44:a7:d9
phy name        :port20
bank_id         :3
phy_addr        :0x64
lane            :3
sw_port         :36
sw_np_port      :16
vid_phy[6]      :[0x0d][0x41][0x00][0x00][0x00][0x00]
vid_fwd[6]      :[0x00][0x40][0x00][0x00][0x00][0x00]
oid_fwd[6]      :[0x00][0xb5][0x00][0x00][0x00][0x00]
========== Link Status ==========
Admin           :up
netdev status   :up
autonego_setting:1
link_setting    :1
link_speed      :1000
link_duplex     :0
Speed           :1000
Duplex          :Full
link_status     :Up
rx_link_status  :0
int_phy_link    :0
local_fault     :0
local_warning   :0
remote_fault    :0
```

Figura 38: Puerto 20 – Diagnostico

Fuente: Elaboración propia

3.3.3 Pruebas de Conectividad Básica

A continuación se detallará paso a paso cada prueba a realizarse. Como se visualiza en la Figura 39, se realizó un test de conectividad hacia Internet por IP y por DNS, donde no se verificó pérdida de paquetes de datos ni latencia en la navegación en la página web.

```
FGT-UNT # execute ping 200.62.191.11
PING 200.62.191.11 (200.62.191.11): 56 data bytes
64 bytes from 200.62.191.11: icmp_seq=0 ttl=251 time=7.7 ms
64 bytes from 200.62.191.11: icmp_seq=1 ttl=251 time=7.7 ms
64 bytes from 200.62.191.11: icmp_seq=2 ttl=251 time=7.7 ms
64 bytes from 200.62.191.11: icmp_seq=3 ttl=251 time=7.7 ms
64 bytes from 200.62.191.11: icmp_seq=4 ttl=251 time=7.7 ms

--- 200.62.191.11 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.7/7.7/7.7 ms

FGT-UNT # execute ping google.com.pe
PING google.com.pe (74.125.141.94): 56 data bytes
64 bytes from 74.125.141.94: icmp_seq=0 ttl=252 time=105.4 ms
64 bytes from 74.125.141.94: icmp_seq=1 ttl=252 time=105.4 ms
64 bytes from 74.125.141.94: icmp_seq=2 ttl=252 time=105.4 ms
64 bytes from 74.125.141.94: icmp_seq=3 ttl=252 time=105.4 ms
64 bytes from 74.125.141.94: icmp_seq=4 ttl=252 time=105.4 ms

--- google.com.pe ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 105.4/105.4/105.4 ms

FGT-UNT #
```

Figura 39: Conectividad hacia la Página Google, por IP y DNS.

Fuente: Elaboración propia.

3.3.4 Pruebas de Publicación

El objetivo de las pruebas de servicios publicados es validar que pueden ser accedidos desde fuera de la red de la Universidad Nacional de Trujillo solo con los puertos específicos.

Como se muestra en la Figura 40, se realiza prueba con el servicio web de la Oficina General de Admisión de la Universidad Nacional de Trujillo, Acceso a las direcciones de NAT (VIP - Virtual IP)

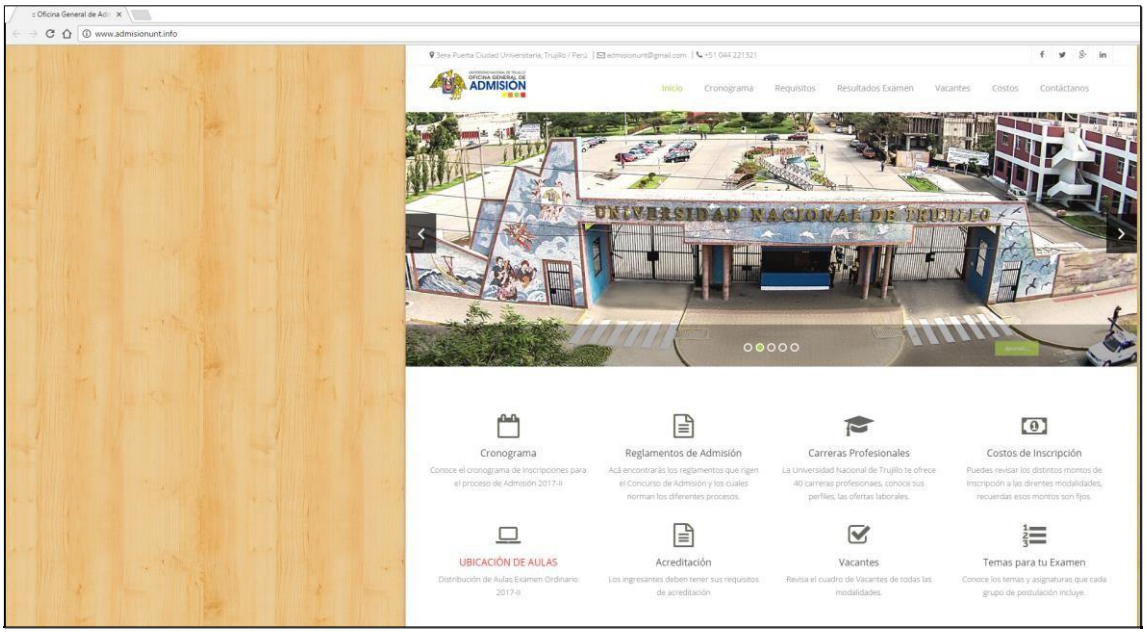


Figura 40: Oficina General de Adminision de la Universidad Nacional de Trujillo

Fuente: http://www.admisionunt.info/

En la Figura 41, se muestra la conectividad de una PC, fuera de la red academica de la entidad, hacia la pagina web “admisionunt.info” de la Oficina General de Admision de la Universidad Nacional de Trujillo.

```
C:\Users\user>ping admisionunt.info

Haciendo ping a admisionunt.info [50.87.201.131] con 32 bytes de datos:
Respuesta desde 50.87.201.131: bytes=32 tiempo=173ms TTL=49
Respuesta desde 50.87.201.131: bytes=32 tiempo=175ms TTL=49
Respuesta desde 50.87.201.131: bytes=32 tiempo=173ms TTL=49
Respuesta desde 50.87.201.131: bytes=32 tiempo=170ms TTL=46

Estadísticas de ping para 50.87.201.131:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 170ms, Máximo = 175ms, Media = 172ms

C:\Users\user>
```

Figura 41: Conectividad a la web admisionunt.info

Fuente: Elaboracion propia.

3.3.5 Pruebas de Política (Acceso a servicios)

En la figura 42, se evidencia el filtro web y los controles de aplicación asignados en cada política, cumpliendo con el funcionamiento correcto.

user=raparicio | Device: All Devices | Last 4 hours | GO | Custom Vie

#	Date/Time	Device ID	Action	Source/Device	Destination IP	Service	Sent/Received	User
1	15:50:36	FWF60C3G11002065	close	192.168.1.68	66.196.66.156	HTTPS	272 B / 112 B	raparicio
2	15:50:33	FWF60C3G11002065	close	192.168.1.68	208.91.113.80	POP3	168 B / 192 B	raparicio
3	15:50:26	FWF60C3G11002065	timeout	192.168.1.68	192.168.5.11	SAMBA	64 B / 0	raparicio
4	15:50:26	FWF60C3G11002065	timeout	192.168.1.68	192.168.5.11	SMB	64 B / 0	raparicio
5	15:50:26	FWF60C3G11002065	timeout	192.168.1.68	192.168.25.1	SAMBA	64 B / 0	raparicio
6	15:50:26	FWF60C3G11002065	timeout	192.168.1.68	192.168.25.1	SMB	64 B / 0	raparicio
7	15:50:26	FWF60C3G11002065	close	192.168.1.68	208.91.113.80	POP3	168 B / 192 B	raparicio
8	15:50:19	FWF60C3G11002065	close	192.168.1.68	208.91.113.80	POP3	168 B / 192 B	raparicio
9	15:49:53	FWF60C3G11002065	close	192.168.1.68	208.91.113.80	POP3	168 B / 192 B	raparicio
10	15:48:42	FWF60C3G11002065	close	192.168.1.68	17.151.227.12	HTTPS	184 B / 84 B	raparicio
11	15:48:15	FWF60C3G11002065	close	192.168.1.68	66.196.66.156	HTTPS	208 B / 88 B	raparicio
12	15:48:15	FWF60C3G11002065	close	192.168.1.68	66.196.66.156	HTTPS	208 B / 88 B	raparicio
13	15:48:15	FWF60C3G11002065	close	192.168.1.68	66.196.66.156	HTTPS	208 B / 88 B	raparicio
14	15:48:14	FWF60C3G11002065	close	192.168.1.68	66.196.66.212	HTTPS	168 B / 88 B	raparicio
15	15:48:11	FWF60C3G11002065	timeout	192.168.1.68	192.168.5.11	SAMBA	64 B / 0	raparicio
16	15:48:11	FWF60C3G11002065	timeout	192.168.1.68	192.168.5.11	SMB	64 B / 0	raparicio
17	15:48:11	FWF60C3G11002065	timeout	192.168.1.68	192.168.25.1	SAMBA	64 B / 0	raparicio
18	15:48:11	FWF60C3G11002065	timeout	192.168.1.68	192.168.25.1	SMB	64 B / 0	raparicio
19	15:48:06	FWF60C3G11002065	close	192.168.1.68	66.196.66.156	HTTPS	220 B / 112 B	raparicio
20	15:48:06	FWF60C3G11002065	close	192.168.1.68	66.196.66.156	HTTPS	272 B / 112 B	raparicio
21	15:48:06	FWF60C3G11002065	close	192.168.1.68	66.196.66.156	HTTPS	272 B / 112 B	raparicio

Figura 42: Control de acceso hacia Internet

Fuente: Elaboración propia.

CONCLUSIONES

Luego de la implementación de la solución perimetral administrada en la Universidad Nacional de Trujillo se pueden realizar las siguientes conclusiones:

1. La integración de un dispositivo UTM fue una medida adecuada que aumentó la seguridad perimetral de la entidad, proporcionando controles a los administradores de la red para monitoreo y restricción del acceso a la red desde la extranet e incluso la intranet.

2. Se logró independizar la red de datos de los servidores de la entidad de todos los usuarios e invitados de la red, permitiendo únicamente un acceso controlado a los servicios que estos proporcionan a través de la aplicación de políticas de firewall en el UTM, que disminuyen los riesgos de seguridad asociados.

3. Se habilitó el uso de un canal de datos dedicado para acceso a internet que la entidad no había logrado usar con la funcionalidad adicional de ser un canal de respaldo ante el fallo del canal de datos principal.

4. Se logró restringir y controlar la navegación que los usuarios realizan hacia internet y con esto se garantiza un uso adecuado del recurso informático constituido por el servicio de internet y la disminución de los riesgos asociados a una navegación descontrolada hacia sitios públicos.

5. Se logró la instalación adecuada del firewall para el control de la seguridad perimetral de la Universidad Nacional de Trujillo.

6. No se realizó la segmentación de una DMZ, ya que la entidad indicó que luego de migrar algunos servidores web internos hacia el data center, se solicitará la creación de dicha red de servidores.

RECOMENDACIONES

A pesar de los controles que se han establecido con la implementación del dispositivo UTM de FortiGate 1500 D, en la red de la Universidad Nacional de Trujillo, se realizan las siguientes recomendaciones a la entidad:

1. Redacción y divulgación de una política de seguridad informática al interior de la entidad que especifique y describa los controles que se deben realizar en la administración de los recursos informáticos.

2. Incorporación de mecanismos de control adicionales en la intranet como es el caso de uso de VLAN en los dispositivos switch de la entidad para disminuir aún más los riesgos asociados a esta red.

3. Evaluación constante y periódica de los controles a seguridad informática de la entidad para detección temprana de amenazas debido a que los riegos informáticos evolucionan muy rápidamente.

4. Se debe crear conciencia en la alta gerencia de que los riesgos a la seguridad informática representan para la empresa y la necesidad constante de implementación de controles que disminuyan y en lo posible minimicen estos riesgos, para que aprueben y apoyen económicamente las soluciones planteadas.

5. Integrar un directorio activo en la red académica para los usuarios con el fin de asociarlo al equipo FortiGate 1500D, esto facilitará la creación y un mayor control en las políticas de navegación web interno.

6. Para un mayor respaldo del enlace de Internet, se puede adquirir un equipo firewall del mismo modelo para la configuración de la alta disponibilidad (HA). Esto permitirá a la entidad que si por una razón podría fallar el equipo principal, el equipo de contingencia entre en funcionamiento y así no poder alterar el servicio del enlace.

7. Se podrá realizar mejoras en los túneles VPN, colocando un ancho de banda asignado (máximo y mínimo) con la finalidad de no alterar la entrada/salida de la transferencia de datos (archivos) cuando el enlace se encuentre saturado.

8. Realizar en un plazo corto la migración a IPv6, ya que esto se podría obtener una mayor protección en la red académica de la entidad.

BIBLIOGRAFÍA

[1] BARRETO Gustavo Adolfo, Estudio de seguridad en computadoras con sistemas operativos conectados a una red TCP/IP, Universidad del Valle 2001.

[2] VILLALÓN Huerta, Antonio. “Seguridad en Unix y Redes”. Versión 2.1. Julio.

[3] STALLINGS, William. “Comunicaciones y Redes de Computadores”. 7ma Edición. Prentice Hall. New Jersey. 2004.

[4] CANAVAN, John. “Fundamentals of Network Security”. Artech House. United States of America. 2001.

[5] ARGENTINA. ArCERT. “Manual de Seguridad en Redes” [en línea]. 1999. Disponible en Web: http://www.arcert.gov.ar/

[6] MAIWALD, Eric. “Fundamentos de seguridad de redes”. Segunda Edición. McGraw-Hill. 2005.

[7] ZHOW Lidong, Haas Zygmunt J. “Securing Ad Hoc Nectworks”, IEEE Network, Vol. 13, No. 6, pp 24-30, Junio 1999.

[8] Instituto Argentino de Normalización, “Código de práctica para la administración de la seguridad de la información”, IRAM-ISO IEC 17799, Buenos Aires, febrero 2002.

[9] Coordinación de Emergencia en Redes Tele-informáticas de la Administración Pública Argentina, Manual de Seguridad en Redes.

[10] Jesús Herney Cifuentes, César Augusto Narváez, Manual de detección de vulnerabilidades de sistemas operativos en redes TCP/IP, Universidad del Valle 2004.

[11] FORTINET. “FortiGate Unified Threat Management” [en línea]. Disponible en Web:

http://www.fortinet.com/

http://www.fortinet.com/products/fortigate_overvie.html

http://www.fortinet.com/doc/FGT1000-3800DS.pdf

[12] GONCALVES Marcus, “Firewalls Complete”, Mc Graw Hill Beta Books, Cap 6, Enero 1997, Recuperado de Internet: “http://www.ods.com.ua/win/eng/security/firewall/preface.htm”